My Journey 私の旅

Driven by the Inspiration from Hackers in SF Novels

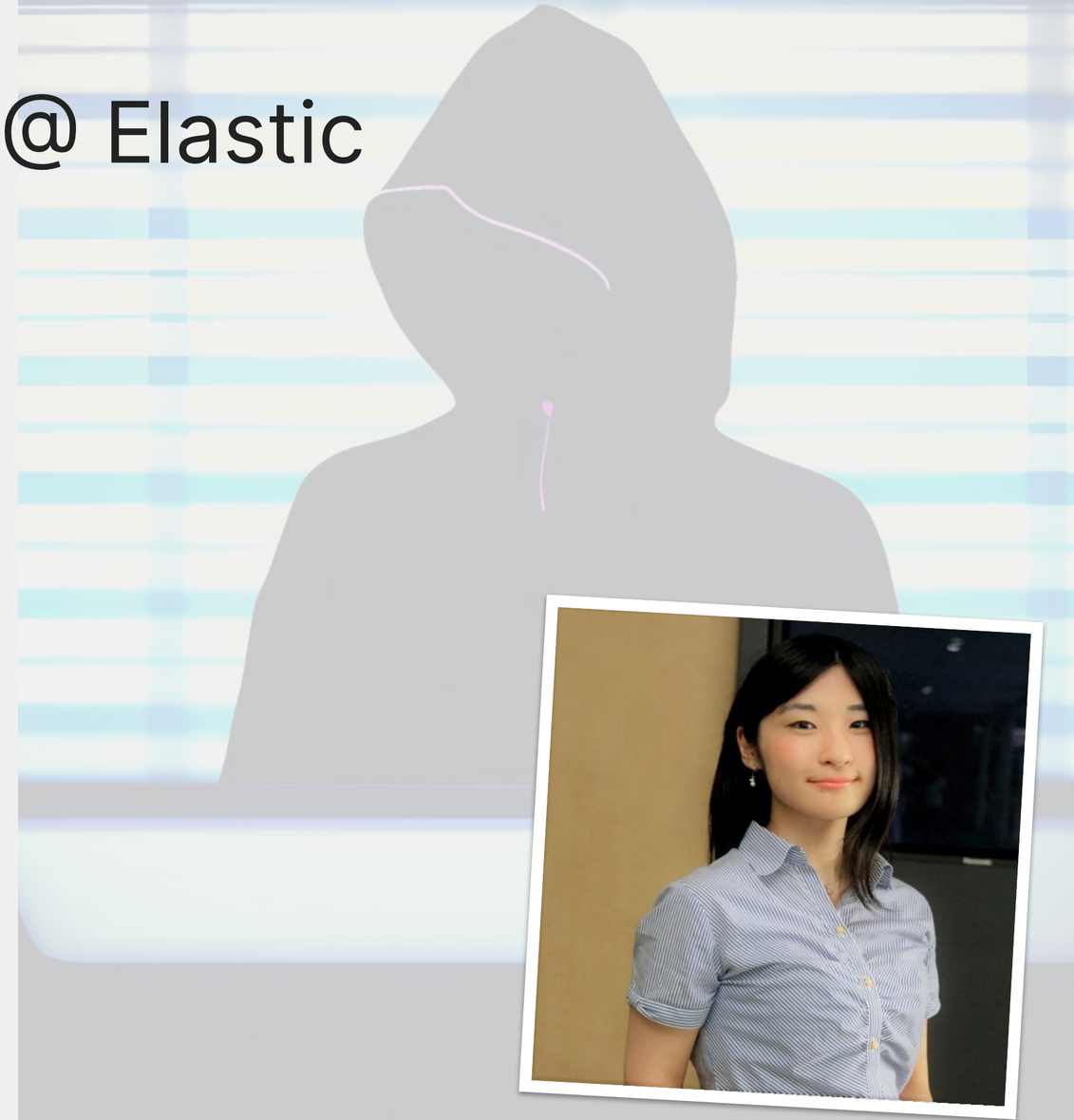
elastic

Asuka Nakajima | 中島 明日香

Security Research Engineer @ Elastic

whoami : Asuka Nakajima

- **Security Research Engineer** @ Elastic



whoami : Asuka Nakajima

- **Security Research Engineer** @ Elastic
- **10+ years** of experience in **Cyber Security R&D**

whoami : Asuka Nakajima

- **Security Research Engineer** @ Elastic
- **10+ years** of experience in **Cyber Security R&D**
- Founded the **first female infosec community in Japan**

whoami : Asuka Nakajima

- **Security Research Engineer** @ Elastic
- **10+ years** of experience in **Cyber Security R&D**
- Founded the **first female infosec community in Japan**
- **BlackHat** USA / Asia Review Board

whoami : Asuka Nakajima

- **Security Research Engineer** @ Elastic
- **10+ years** of experience in **Cyber Security R&D**
- Founded the **first female infosec community in Japan**
- **BlackHat** USA / Asia Review Board
- Published books (**best selling book!**)

Why did you decide to enter this field?

Why did you decide to enter this field?

What motivates you?

Why did you decide to enter this field?

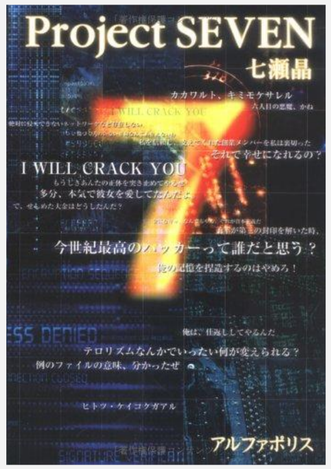
What motivates you?

How did you improve your skills?

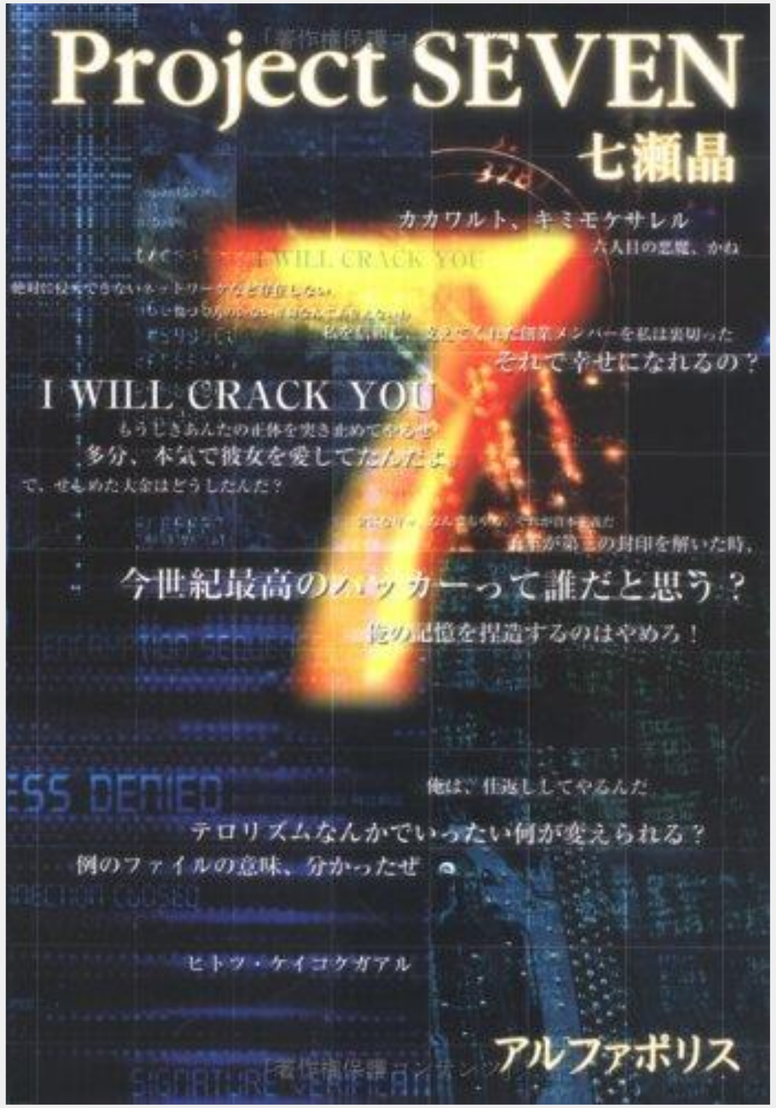
Timeline

Timeline

age 14

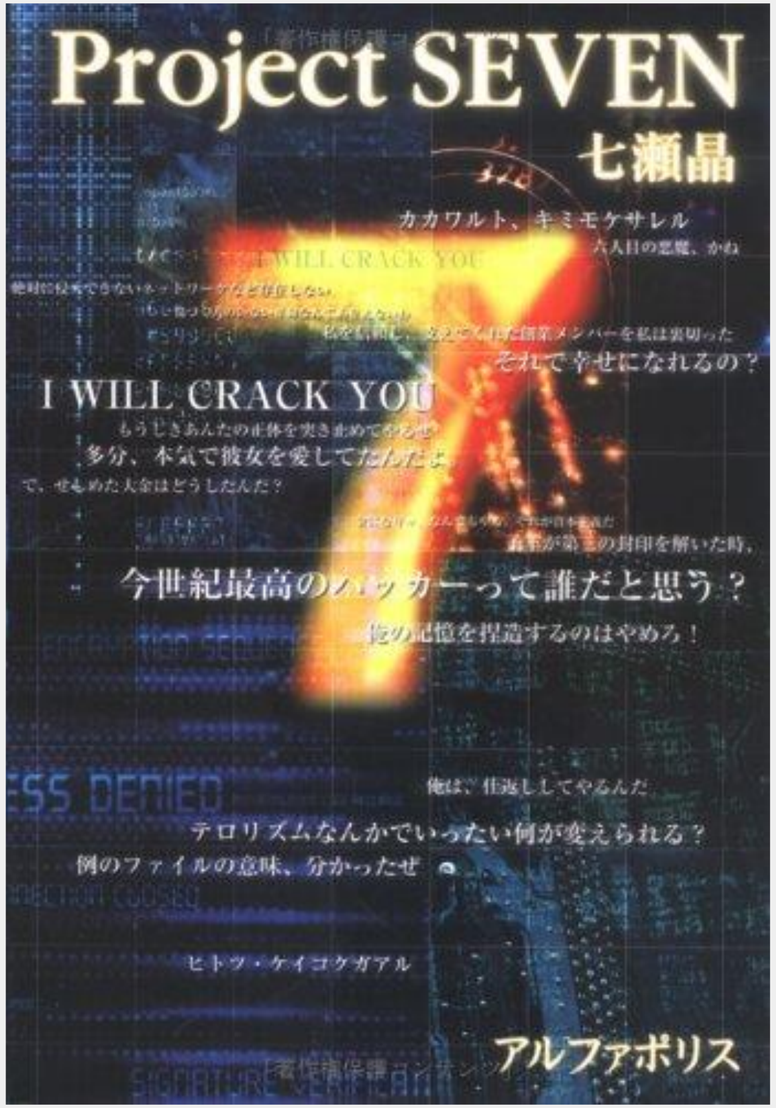


2004



https://www.amazon.co.jp/dp/443406732X

A **high school girl hacker**👩‍💻 and a programmer **saving the world**🌎 from cyber-terrorists



https://www.amazon.co.jp/dp/443406732X

A **high school girl hacker**👩‍💻 and a programmer **saving the world**🌎 from cyber-terrorists

Hackers are so cool!!!

Started studying computers and security on my own👩‍💻

I knew almost nothing about computers..□

謎

Reading a book like “How to use hacking tools” 😢

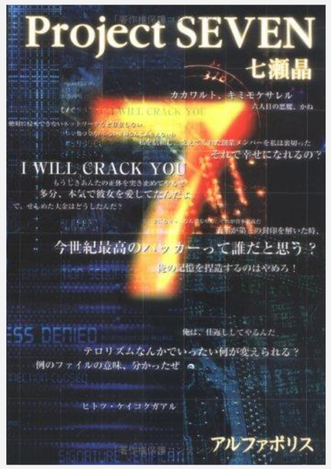
Reading a book like “How to use hacking tools” 😢

Wanted to study advanced topics, **even though I didn’t understand basics yet..**

I started with studying for a **beginner level IT certification** to **learn the basics**

Timeline

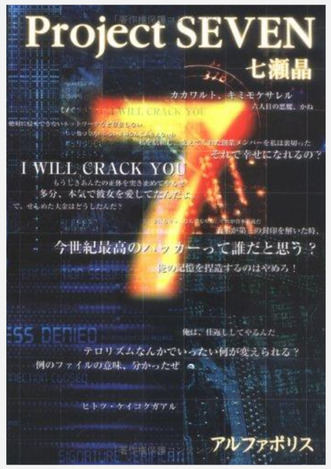
age 14



2004

Timeline

age 14



2004

University Days

DEFCON

2009

Enrolled Keio University

Belonged to the laboratory of a leading IDS (Intrusion Detection System) researcher in Japan

https://www.keio.ac.jp/ja/assets/images/about/campus/sfc/slide/pic_01.jpg

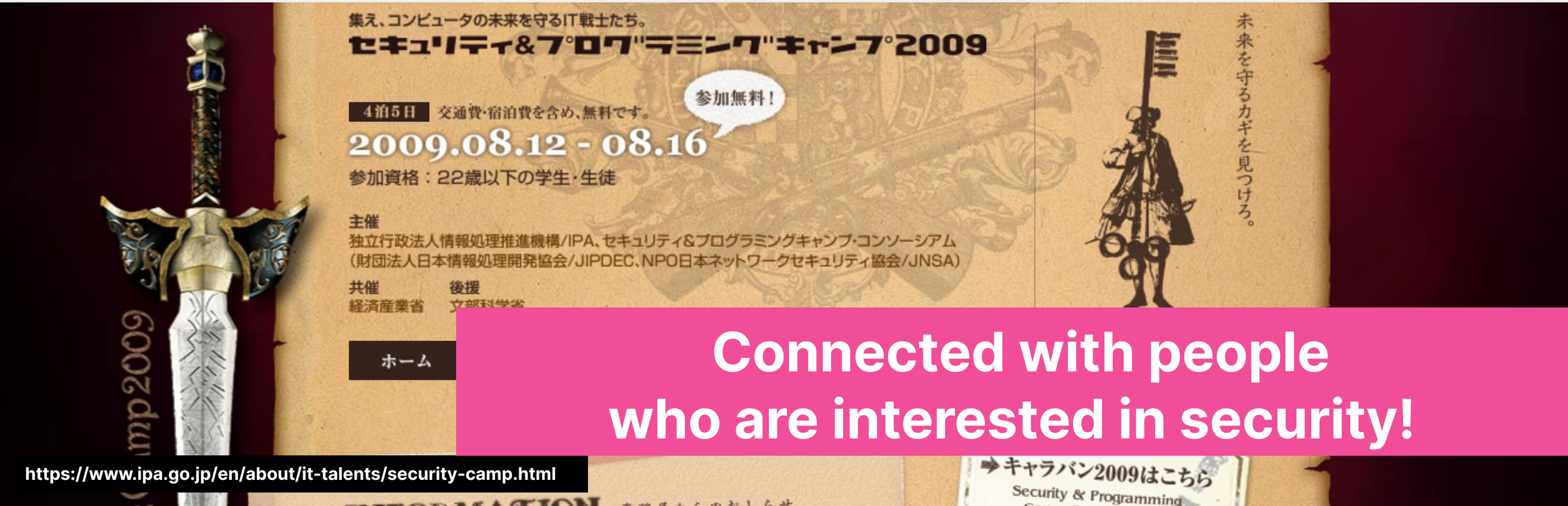
Enrolled Keio University

Belonged to the laboratory of a leading IDS (Intrusion Detection System) researcher in Japan

https://www.keio.ac.jp/ja/assets/images/about/campus/sfc/slide/pic_01.jpg

Participated Security Camp

Multi-day group training programs
for selected students throughout Japan



**Connected with people
who are interested in security!**

https://www.ipa.go.jp/en/about/it-talents/security-camp.html

Joined a CTF team: sutegoma2

DEF CON CTF Finals

Las Vegas, 2011

#2

I couldn’t solve any of the challenges 😢

#2

I couldn’t solve any of the challenges 😢

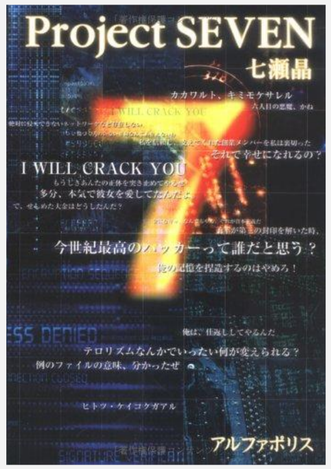
Even though I had passed Japan's most difficult information security national qualification, **there was so much I didn't know**😲

Understood the World Class Level🌎

and, realized that I was quite far from the top level...

Timeline

age 14



2004

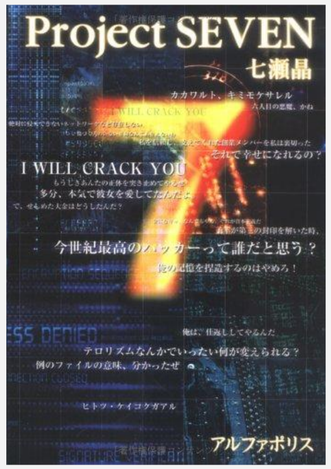
University Days

DEFCON

2009

Timeline

age 14



2004

University Days

DEFCON

2009

Vuln Research

2013

Started my career as a

Security Researcher 👩‍🔬

Software Vulnerability Research

Software Vulnerability Research

If I can **find and address vulnerabilities**🕷️in widely-used software before attackers can exploit, it might **help save the world?**🤔

One-Day Vulnerability

One-day Vulnerability

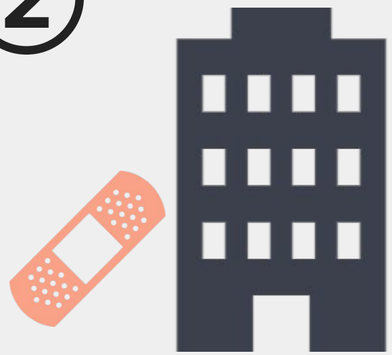
aka N-day Vulnerability

Discovered Unknown Vulnerability

①

Patch / Mitigation Released

②



Applied Patch / Mitigation

③

One-day Vulnerability

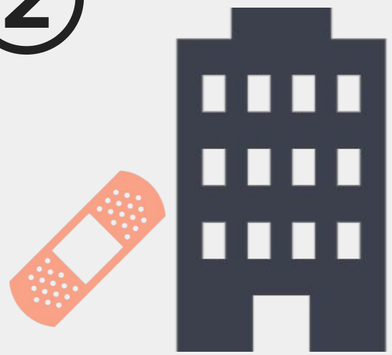
aka N-day Vulnerability

Discovered Unknown Vulnerability

①

Patch / Mitigation Released

②



Applied Patch / Mitigation

③

One-day Vulnerability

aka N-day Vulnerability

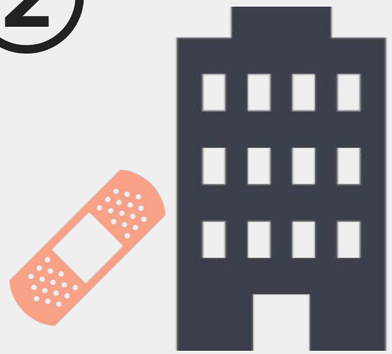
Zero Day

Discovered Unknown Vulnerability

①

Patch / Mitigation Released

②



Applied Patch / Mitigation

③

One-day Vulnerability

aka N-day Vulnerability

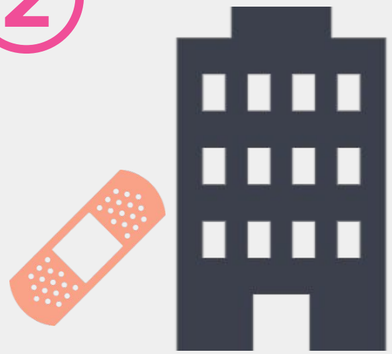
Zero Day

Discovered Unknown Vulnerability

①

Patch / Mitigation Released

②



Applied Patch / Mitigation

③

One-day Vulnerability

aka N-day Vulnerability

Zero Day

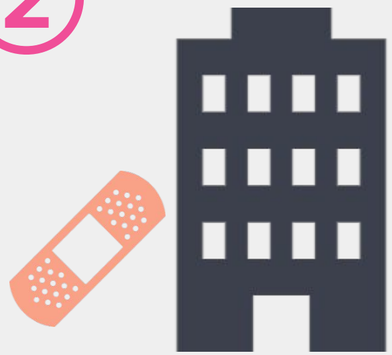
One (N) Day

Discovered Unknown Vulnerability

①

Patch / Mitigation Released

②

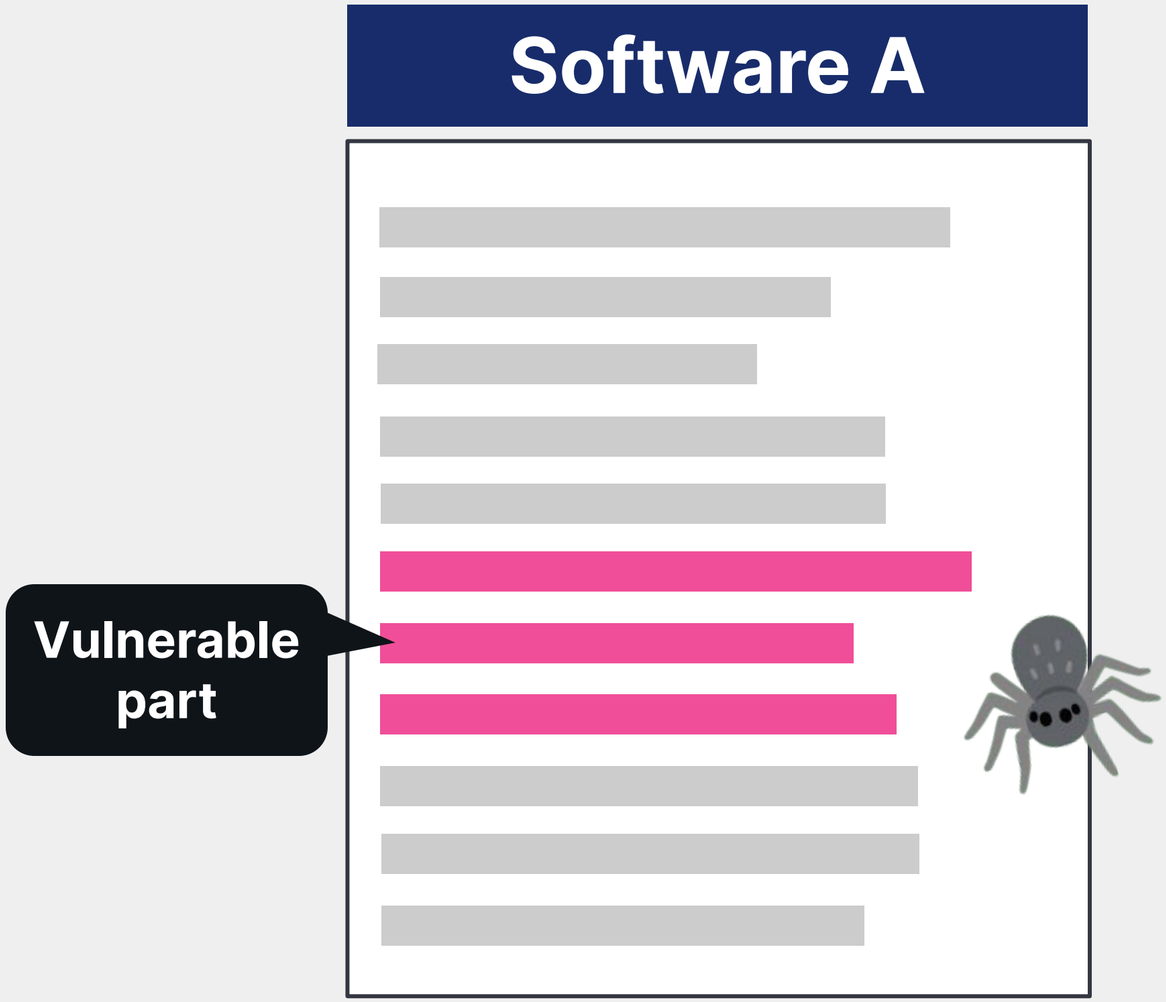


Applied Patch / Mitigation

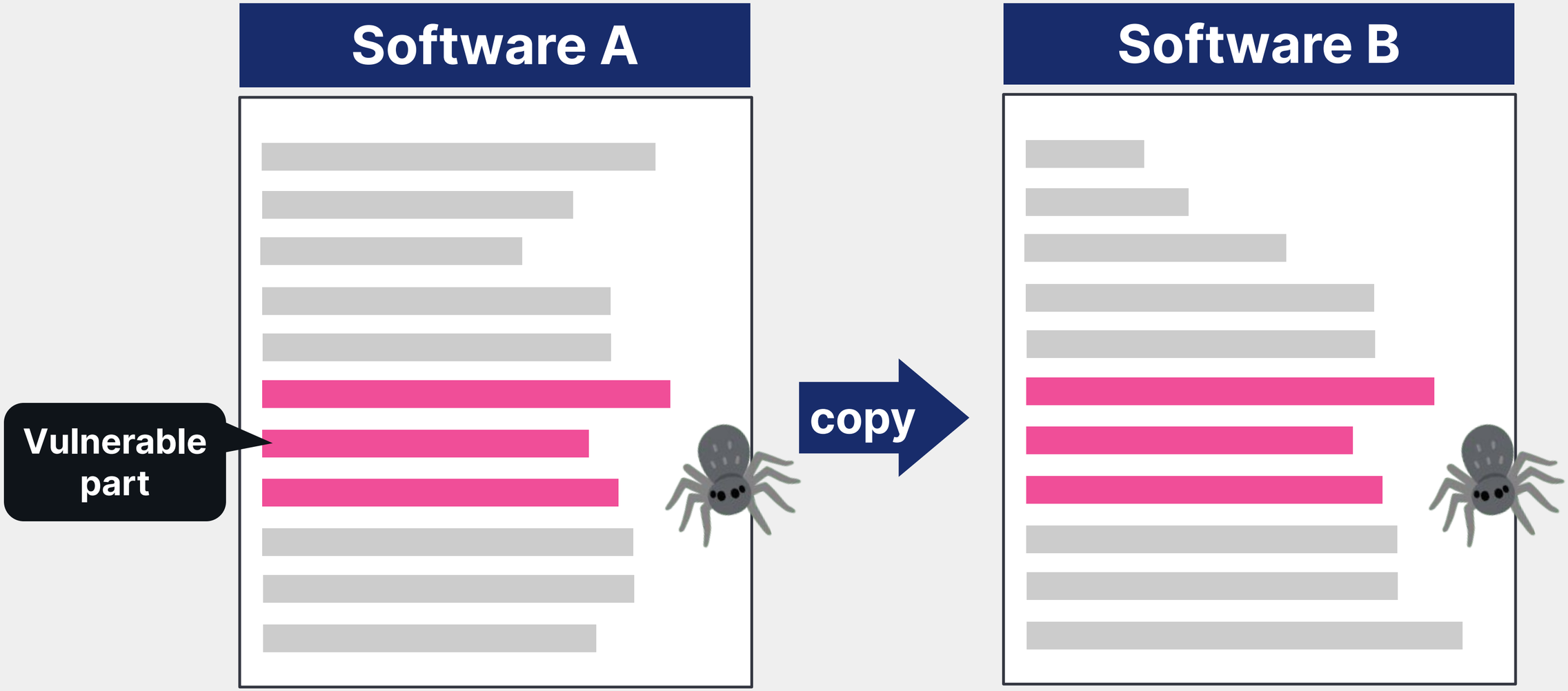
③

Code Clone Vulnerability

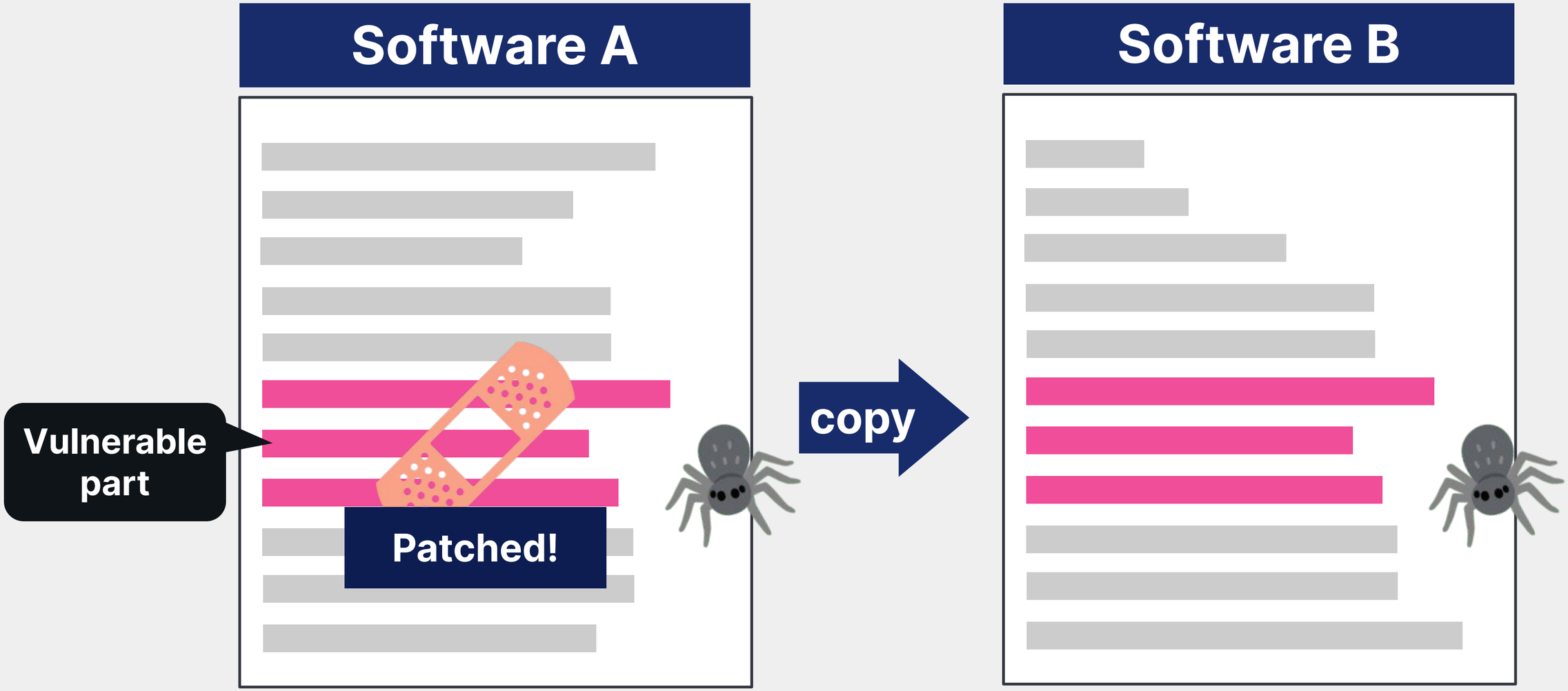
Code Clone Vulnerability



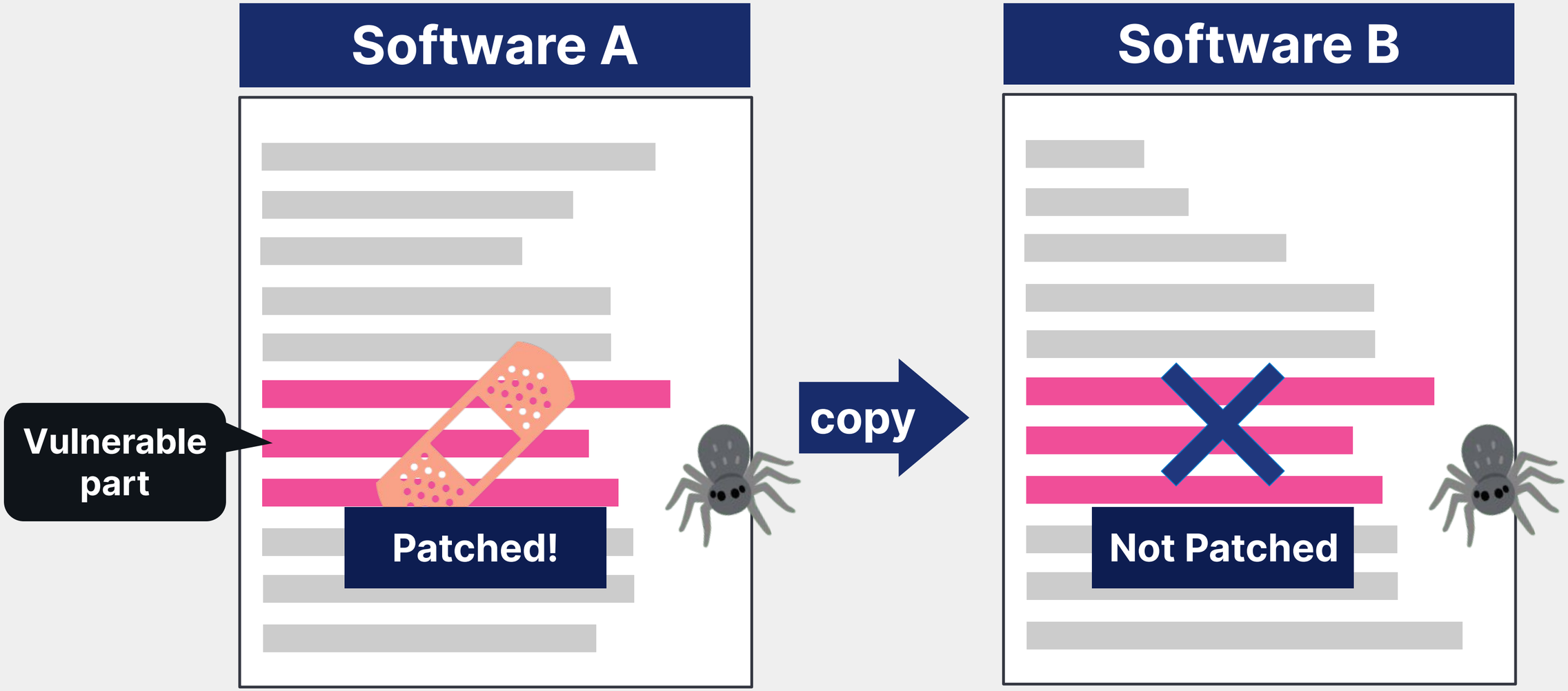
Code Clone Vulnerability



Code Clone Vulnerability



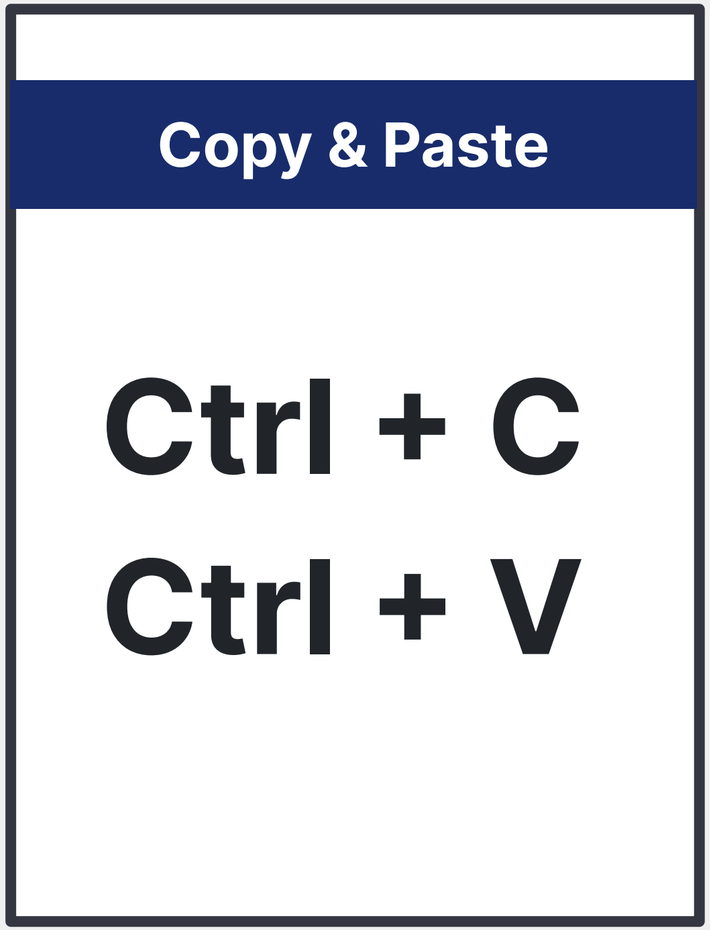
Code Clone Vulnerability



Cloned Vulnerabilities Might Not be Fixed

Why does it Happen?

Why does it Happen?



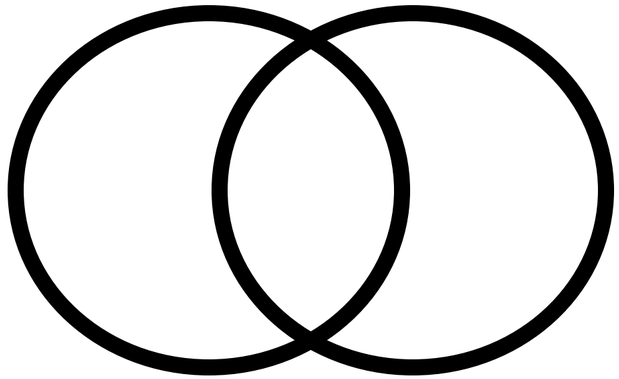
Why does it Happen?

Copy & Paste

Ctrl + C

Ctrl + V

Source Code Sharing



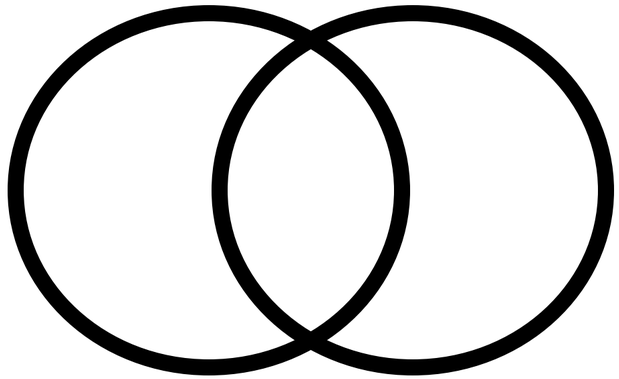
Why does it Happen?

Copy & Paste

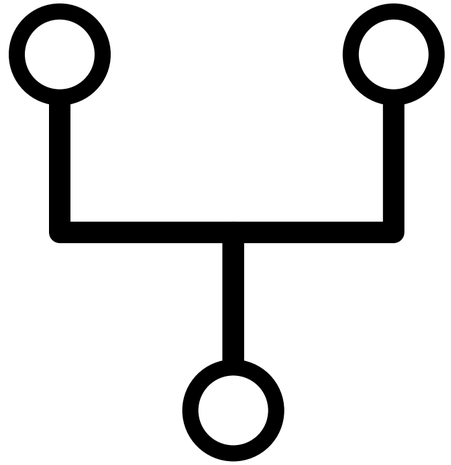
Ctrl + C

Ctrl + V

Source Code Sharing

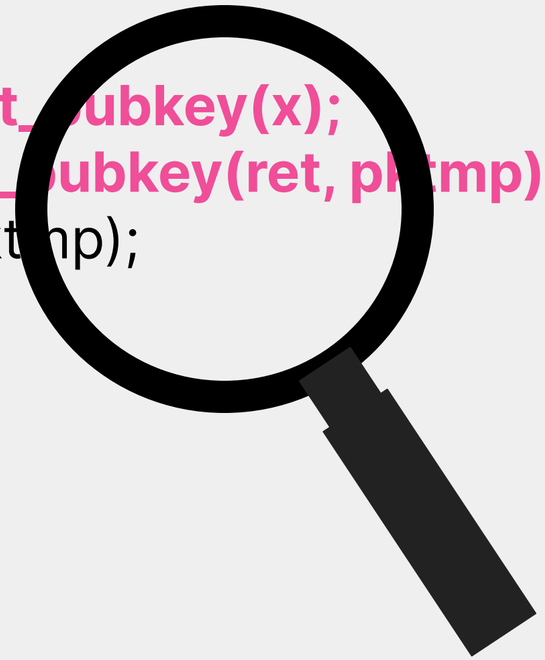


Fork

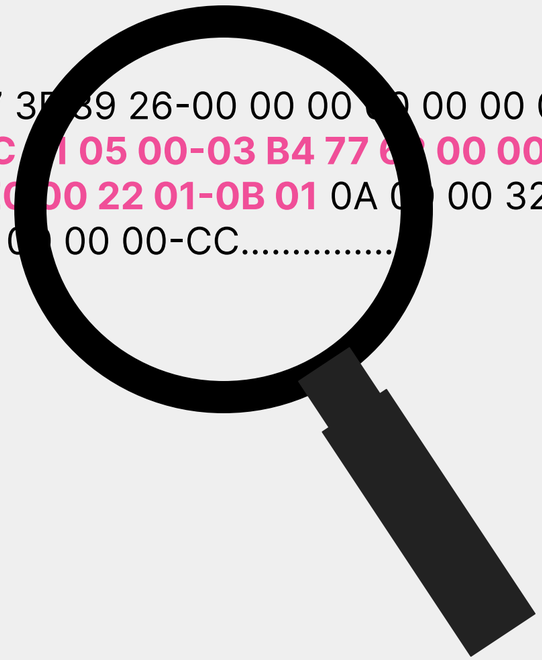


Code Clone Search (2014)

```
pktmp = X509_get_pubkey(x);
i = X509_REQ_set_pubkey(ret, pktmp);
EVP_PKEY_free(pktmp);
.....
```



```
00:00E0 52 69 63 68 27 3E 39 26-00 00 00 00 00 00 00 00
00:00F0 50 45 00 00 4C 01 05 00-03 B4 77 00 00 00 00 00
00:0100 00 00 00 00 E0 00 22 01-0B 01 0A 00 00 32 04 00
00:0110 00 20 02 00 00 00 00 00-CC.....
```

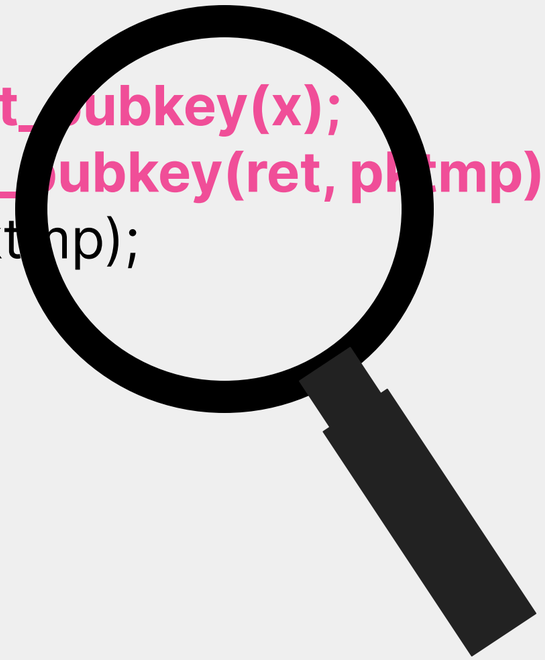


Source Code Based

Binary Based

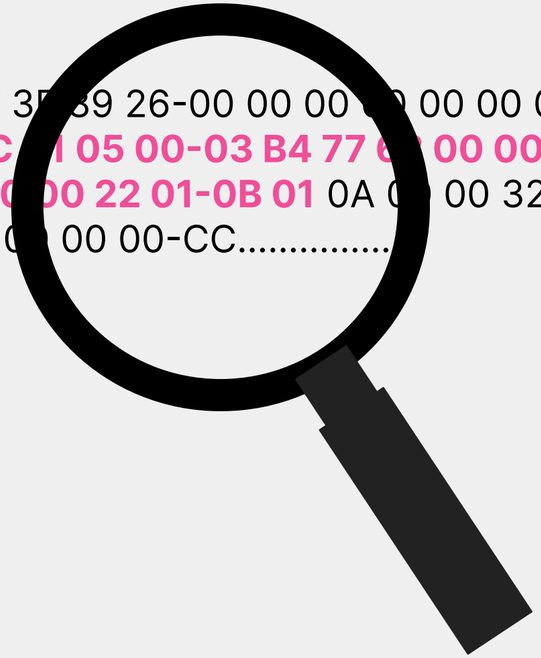
Code Clone Search (2014)

```
pktmp = X509_get_pubkey(x);
i = X509_REQ_set_pubkey(ret, pktmp);
EVP_PKEY_free(pktmp);
.....
```



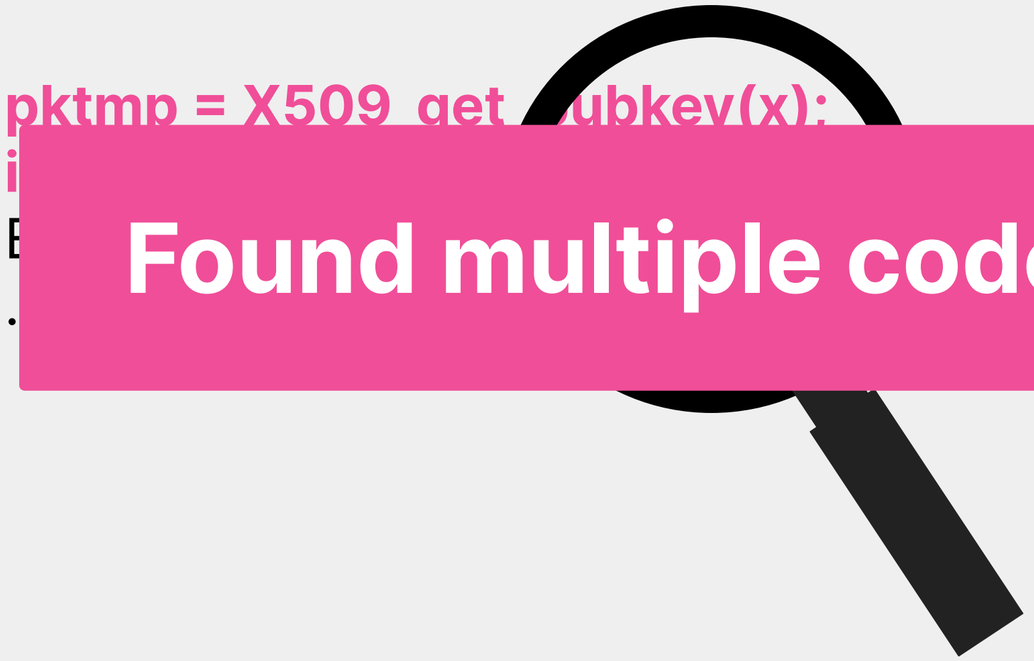
Source Code Based

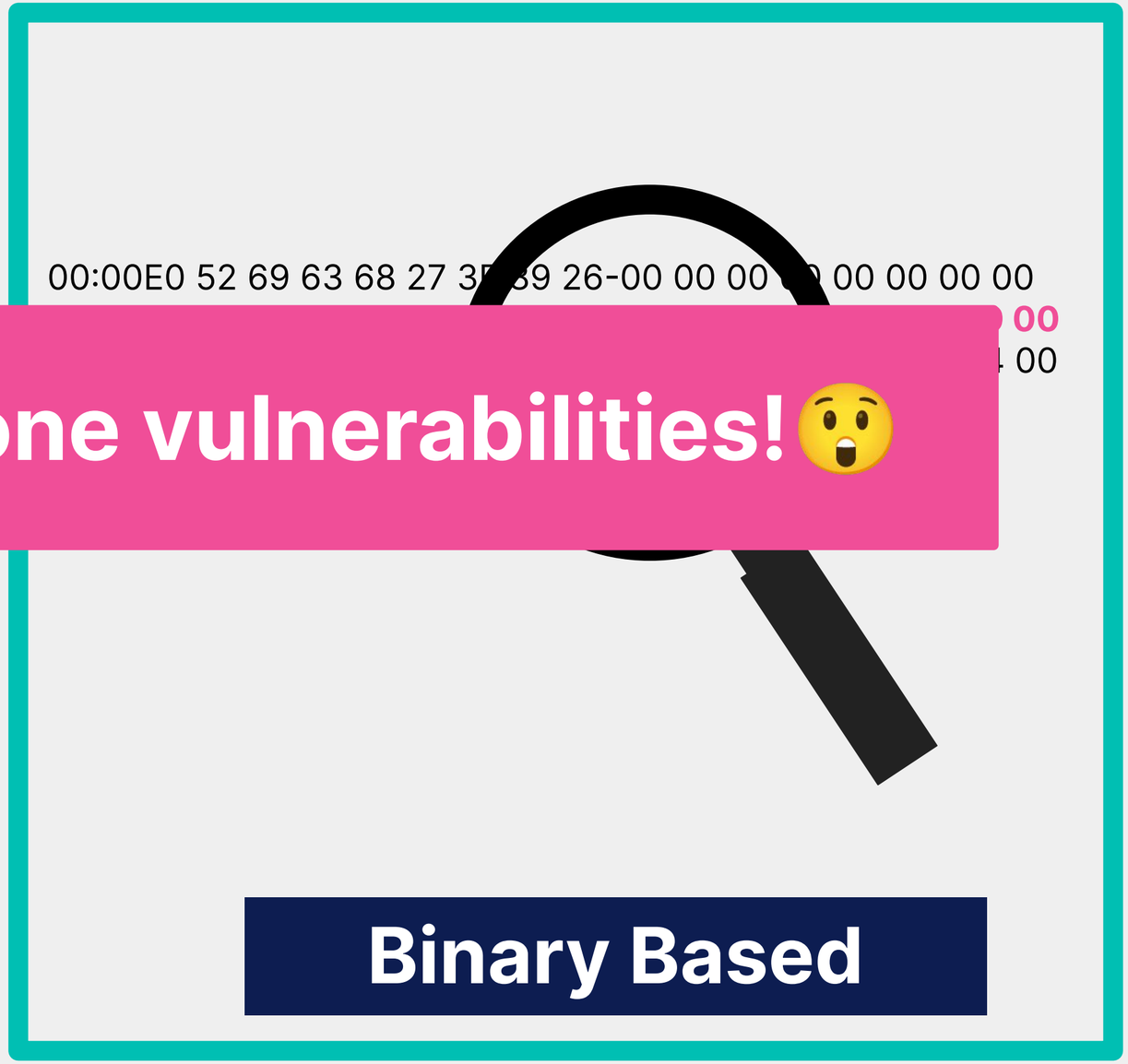
```
00:00E0 52 69 63 68 27 3[illegible]39 26-00 00 00 [illegible]0 00 00 00 00
00:00F0 50 45 00 00 4C [illegible]1 05 00-03 B4 77 [illegible] 00 00 00 00
00:0100 00 00 00 00 E[illegible]0 22 01-0B 01 0A [illegible] 00 32 04 00
00:0110 00 20 02 00 00 [illegible] 00 00-CC.....
```



Binary Based

Code Clone Search (2014)



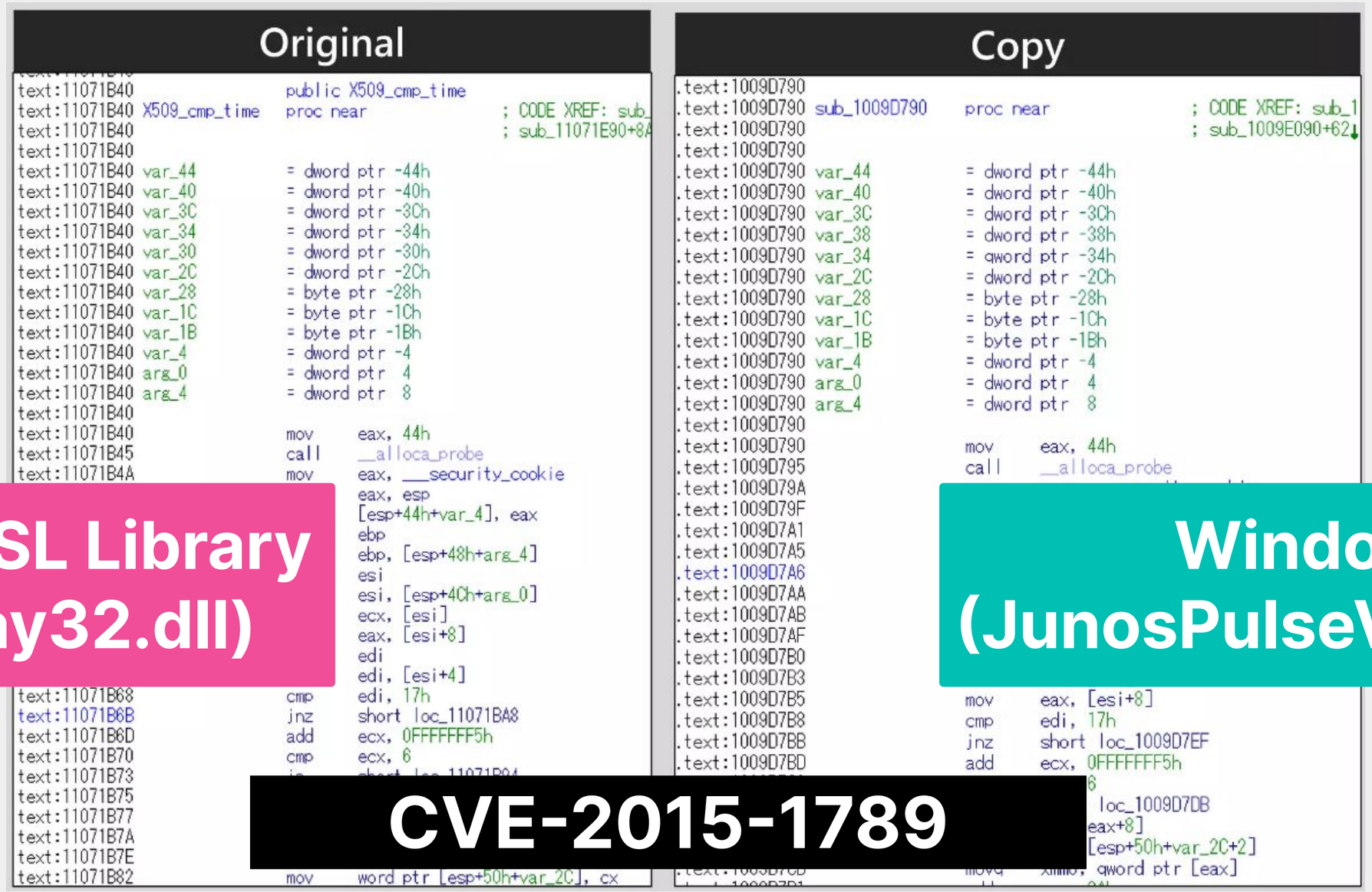


Found multiple codeclone vulnerabilities! 😲

Source Code Based

Binary Based

Found a Code Clone Vulnerability in Windows!



OpenSSL Library (libeay32.dll)

Windows (JunosPulseVpnBg.dll)

CVE-2015-1789

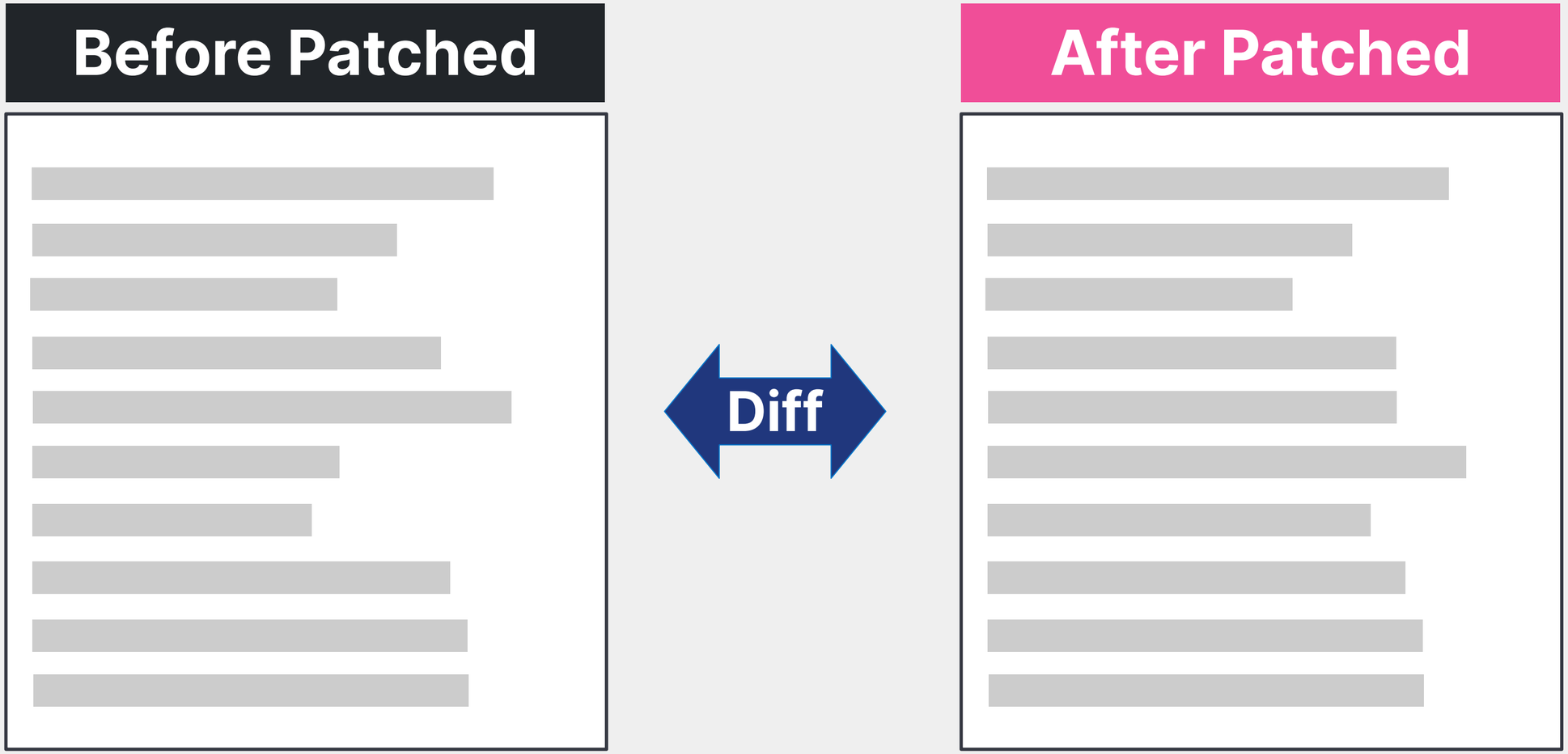
Reference: https://www.slideshare.net/phdays/ss-62579634, p31

Positive Hack Days

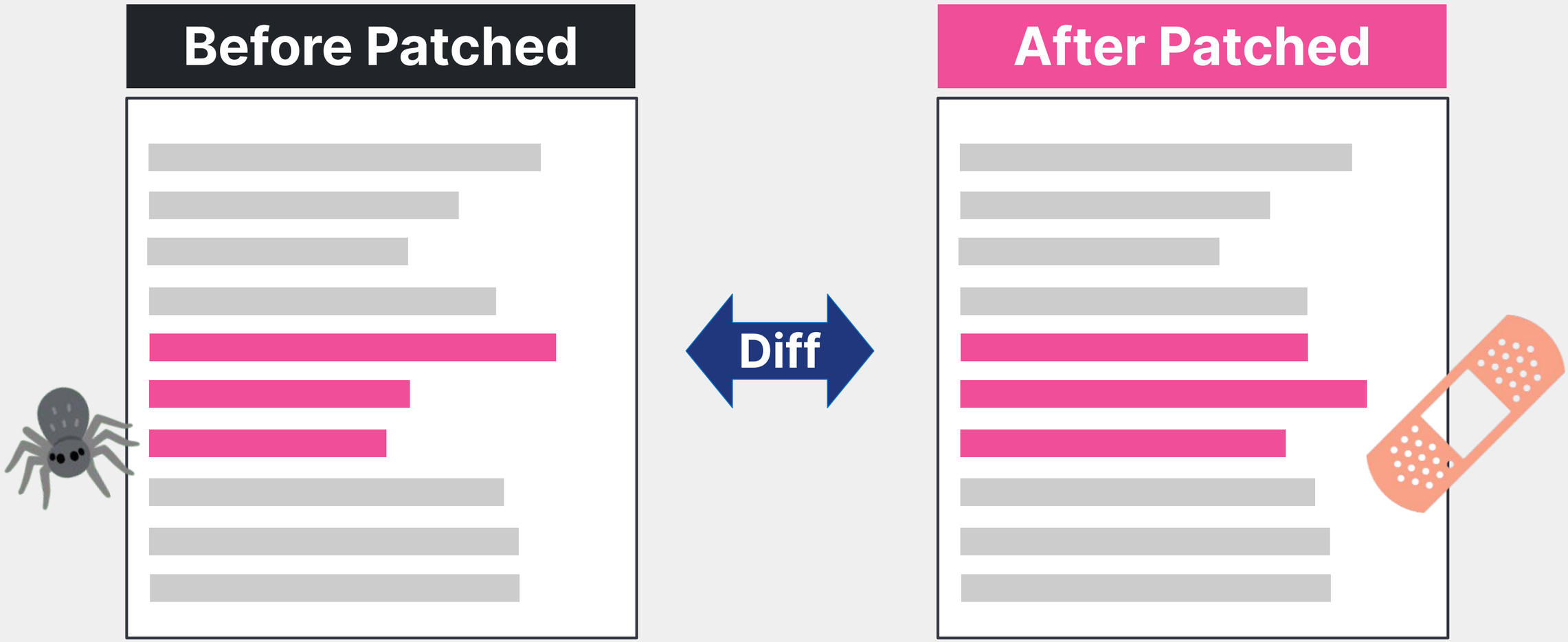
https://www.slideshare.net/phdays/ss-62579634

Patch Diffing Manually to Find the Original Vuln Part

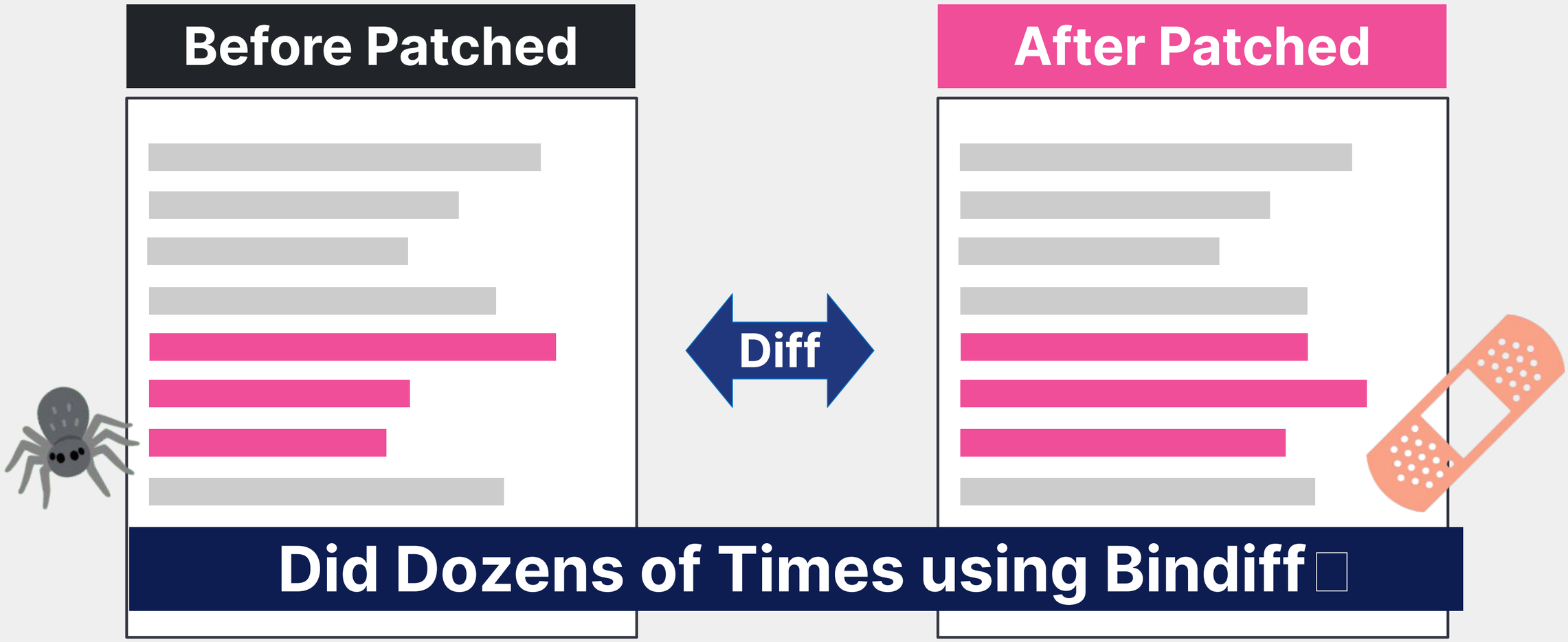
Patch Diffing Manually to Find the Original Vuln Part



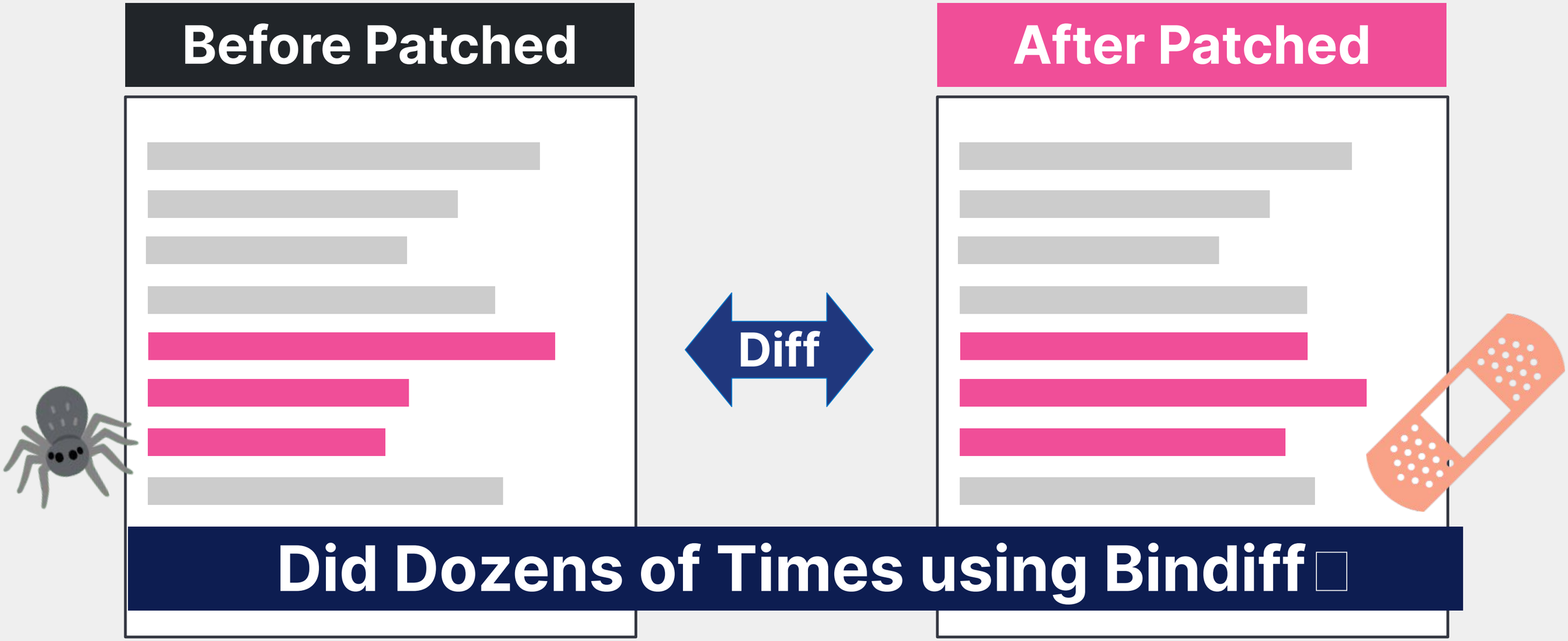
Patch Diffing Manually to Find the Original Vuln Part



Patch Diffing Manually to Find the Original Vuln Part

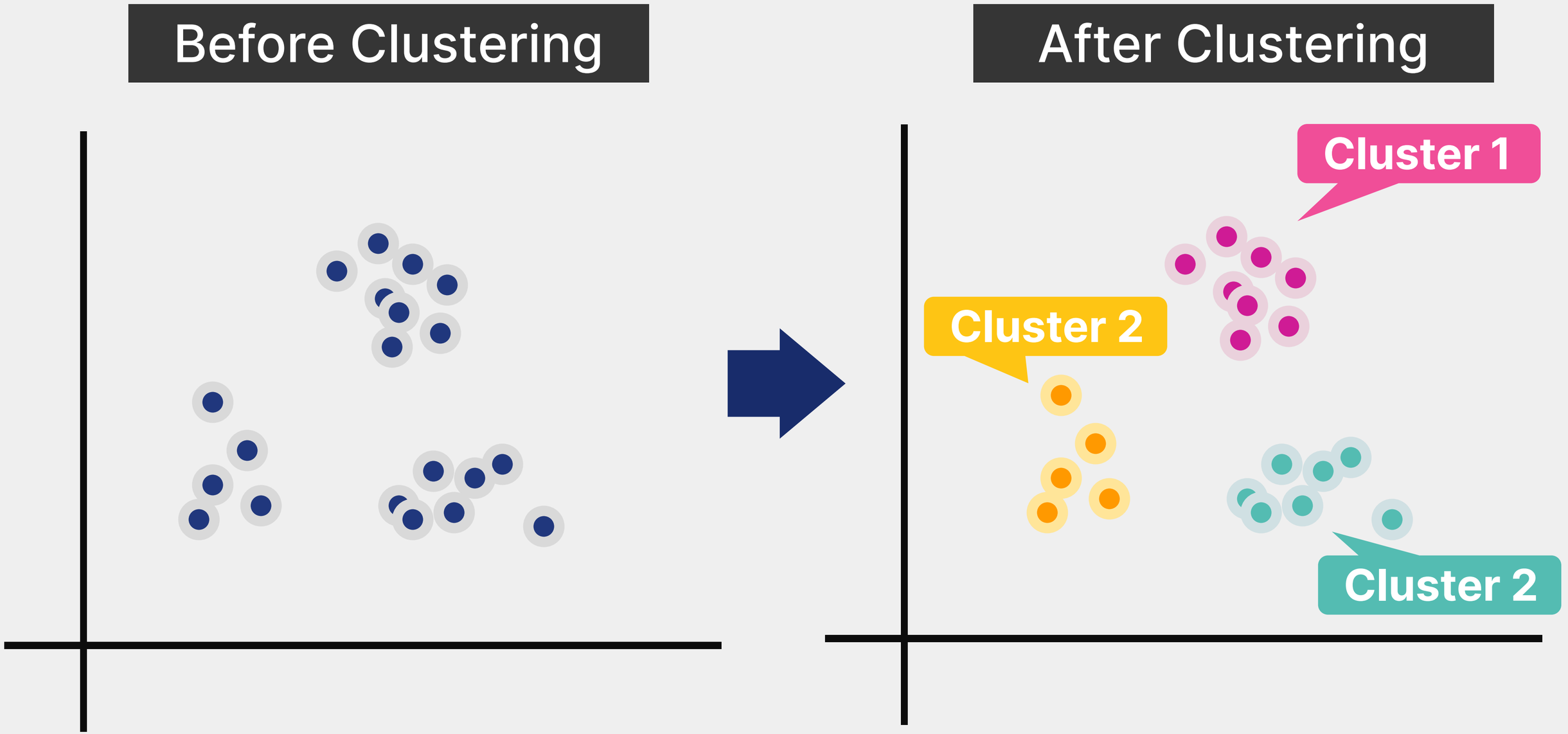


Patch Diffing Manually to Find the Original Vuln Part

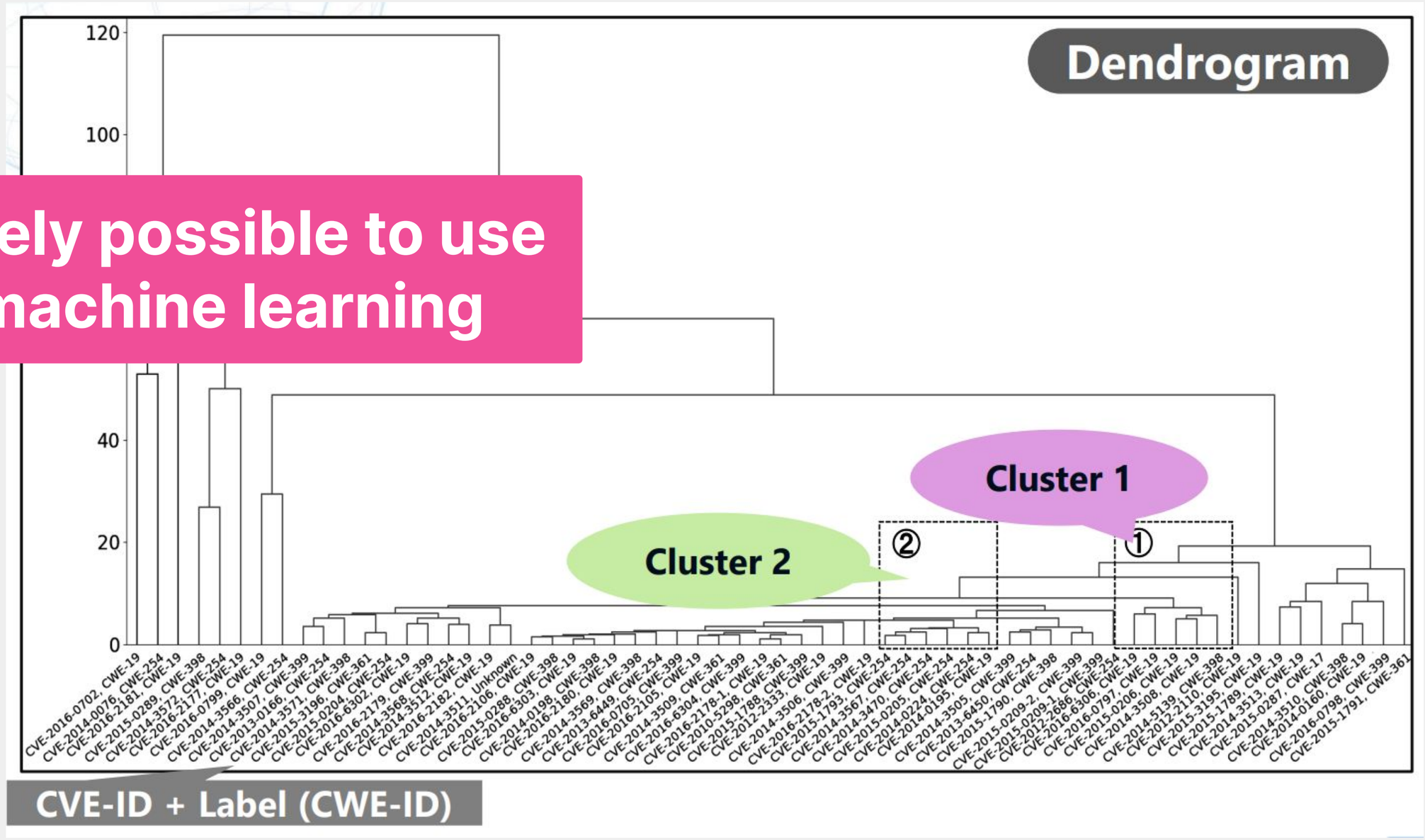


Can Patch Diffing be Facilitated by Using ML?

Clustering

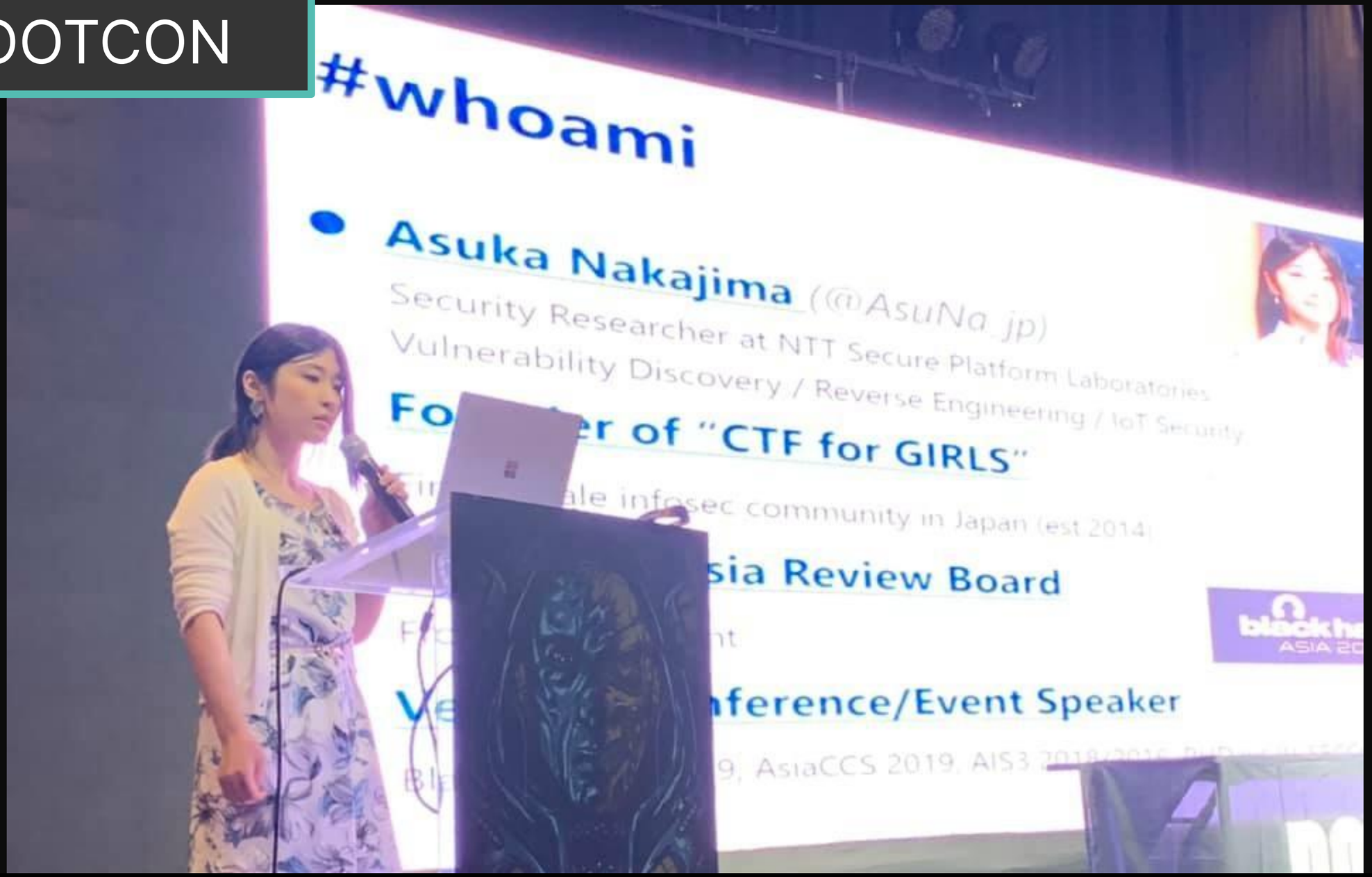

Before Clustering
After Clustering
Cluster 1
Cluster 2
Cluster 2

Found Patterns of Some Types of Vulnerability Fix



https://media.rootcon.org/ROOTCON%2013/Talks/Pilot%20Study%20on%20Semi-Automated%20Patch%20Diffing%20by%20Applying%20Machine-Learning%20Techniques.pdf, p26

ROOTCON



https://media.rootcon.org/ROOTCON%2013/Talks/Pilot%20Study%20on%20Semi-Automated%20Patch%20Diffing%20by%20Applying%20Machine-Learning%20Techniques.pdf

1-Day Vulnerability Risk of IoT Devices

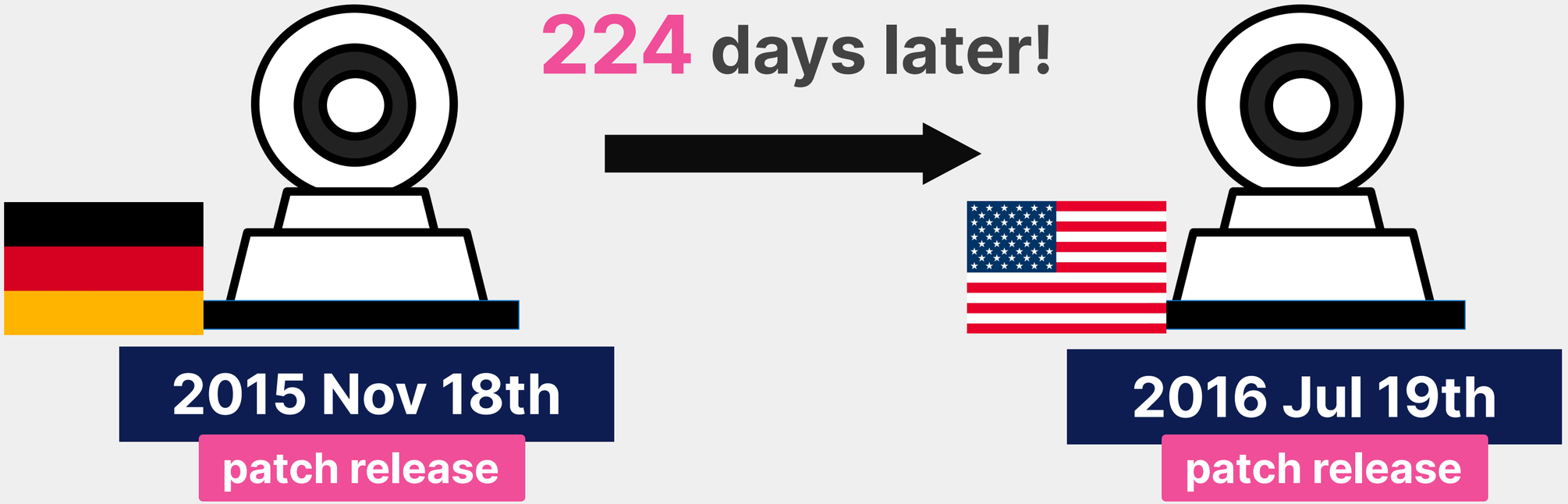
1-Day Vulnerability Risk of IoT Devices

CVE-2017-7852

Vendor D-Link

Model DCS-932L RevA

Unsynchronized Patch Release



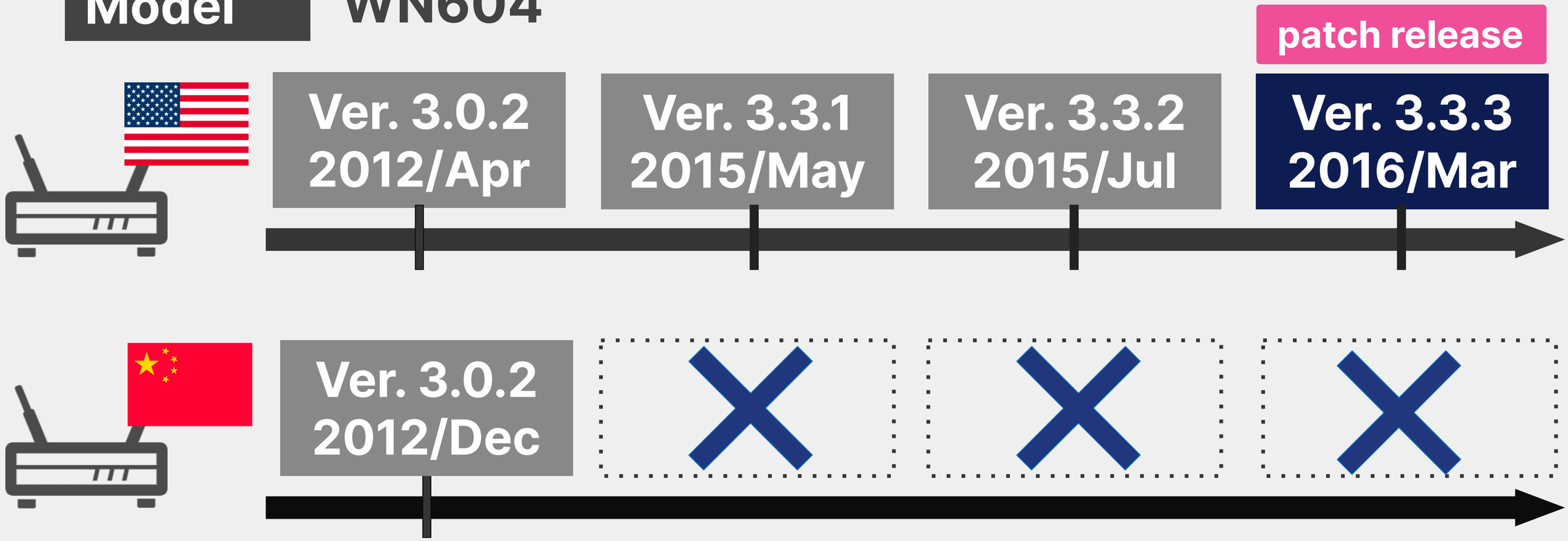
1-Day Vulnerability Risk of IoT Devices

CVE-2016-1556

Vendor Netgear

Model WN604

Implicit End-of-Support (EoS)



ACM Asia CCS

A Pilot Study on Consumer IoT Device Vulnerability Disclosure and Patch Release in Japan and the United States

Asuka Nakajima
NTT Secure Platform Laboratories
asuka.nakajima.db@hco.ntt.co.jp

Takuya Watanabe
NTT Secure Platform Laboratories
takuya.watanabe.yf@hco.ntt.co.jp

Eitaro Shioji
NTT Secure Platform Laboratories
eitaro.shioji.es@hco.ntt.co.jp

Mitsuaki Akiyama
NTT Secure Platform Laboratories
akiyama@ieee.org

Maverick Woo
Carnegie Mellon University
pooh@cmu.edu

ABSTRACT

With our ever increasing dependence on computers, many governments have started to investigate regulations on vulnerabilities and their lifecycle management. Although many previous works have studied this problem space for mainstream software packages and web applications, few studies have targeted consumer IoT devices. As a first step towards filling this void, this paper presents a pilot study on the vulnerability disclosures and patch release behaviors related to 3 prominent consumer IoT vendors in Japan and 3 in the United States. Our goals include (i) characterizing trends and risks using accurate data that spans a long period, and (ii) identifying problems, challenges, and potential approaches for future studies of this problem space. To this end, we collected all published vulnerabilities and their patches for the consumer IoT products by the included vendors between 2006 and 2017; then, we analyzed our [illegible]verity of the vulnerabilities and the timing of patch releases with respect to disclosures

https://dl.acm.org/doi/10.1145/3321705.3329849

9–12, 2019, Auckland, New Zealand. ACM, New York, NY, USA, 8 pages.
https://doi.org/10.1145/3321705.3329849

1 INTRODUCTION

As our society continues to increase its reliance on computers large and small, vulnerabilities and their lifecycle management are gradually becoming a matter of public safety. In response, many governments have started to investigate regulating computer security through legislation/standards setting, e.g., [18, 22]. As we might expect, understanding the past and current practices of the stake-

vulnerabilities, whereas work in the *post-discovery* group focuses

Joint Research with Carnegie Mellon University

#3

Each research took 1~3 years to complete 😲

Each research took 1~3 years to complete 😲

2000 hours & 100+meetings!

#3

Each research took 1~3 years to complete 😲

2000 hours & 100+meetings!

Rejected many times 😢

#3

Each research took 1~3 years to complete 😲

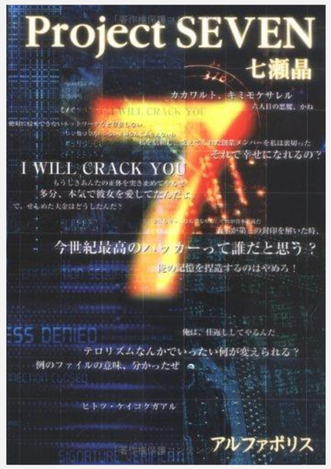
2000 hours & 100+meetings!

Rejected many times 😢

Some research has
not been published... 😞

Timeline

age 14



2004

University Days

DEFCON

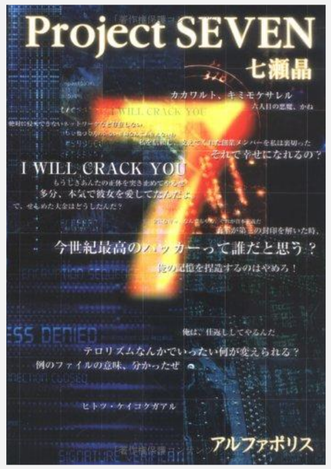
2009

Vuln Research

2013

Timeline

age 14



2004

University Days

DEFCON

2009

Vuln Research

2013

Change the world?

black hat

2019

Security Risk of OEM Supply Chain

aka White Label Model

Security Risk of OEM Supply Chain

aka White Label Model

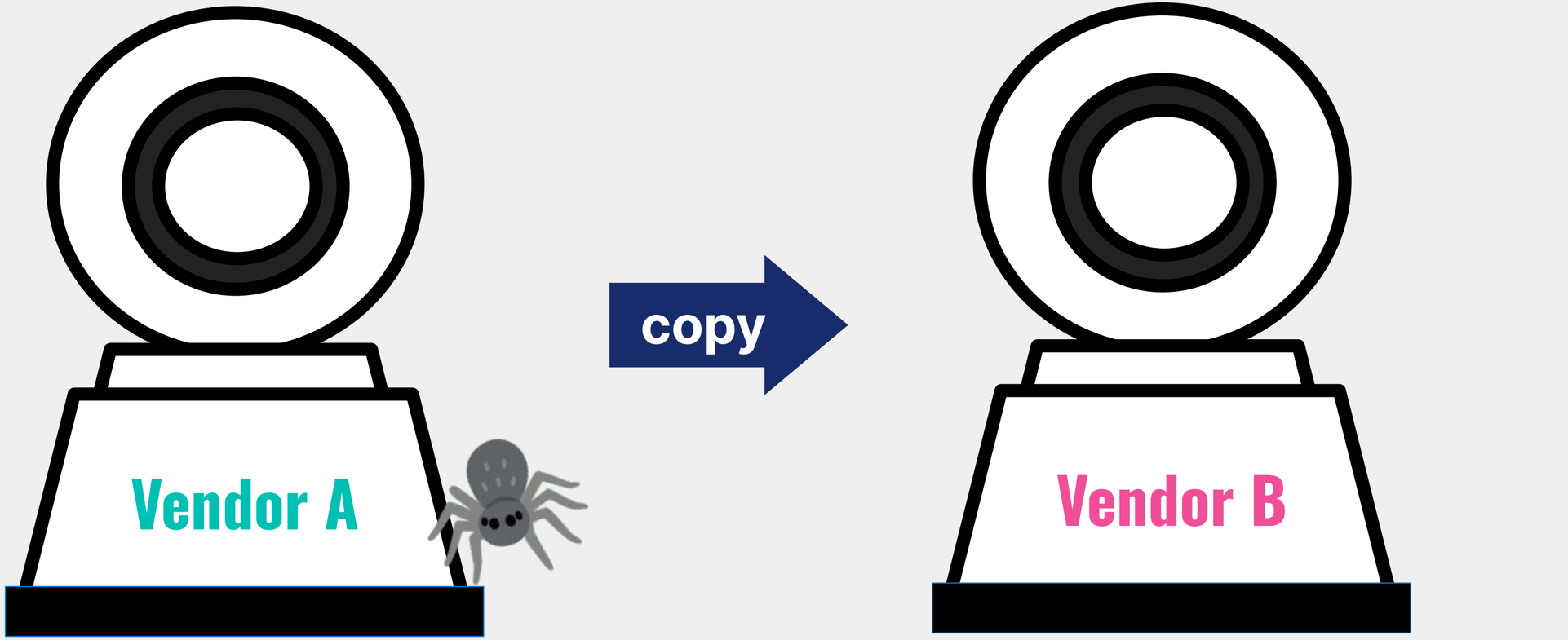
copy

IoT Camera (Original)

IoT Camera (OEM)

Security Risk of OEM Supply Chain

aka White Label Model

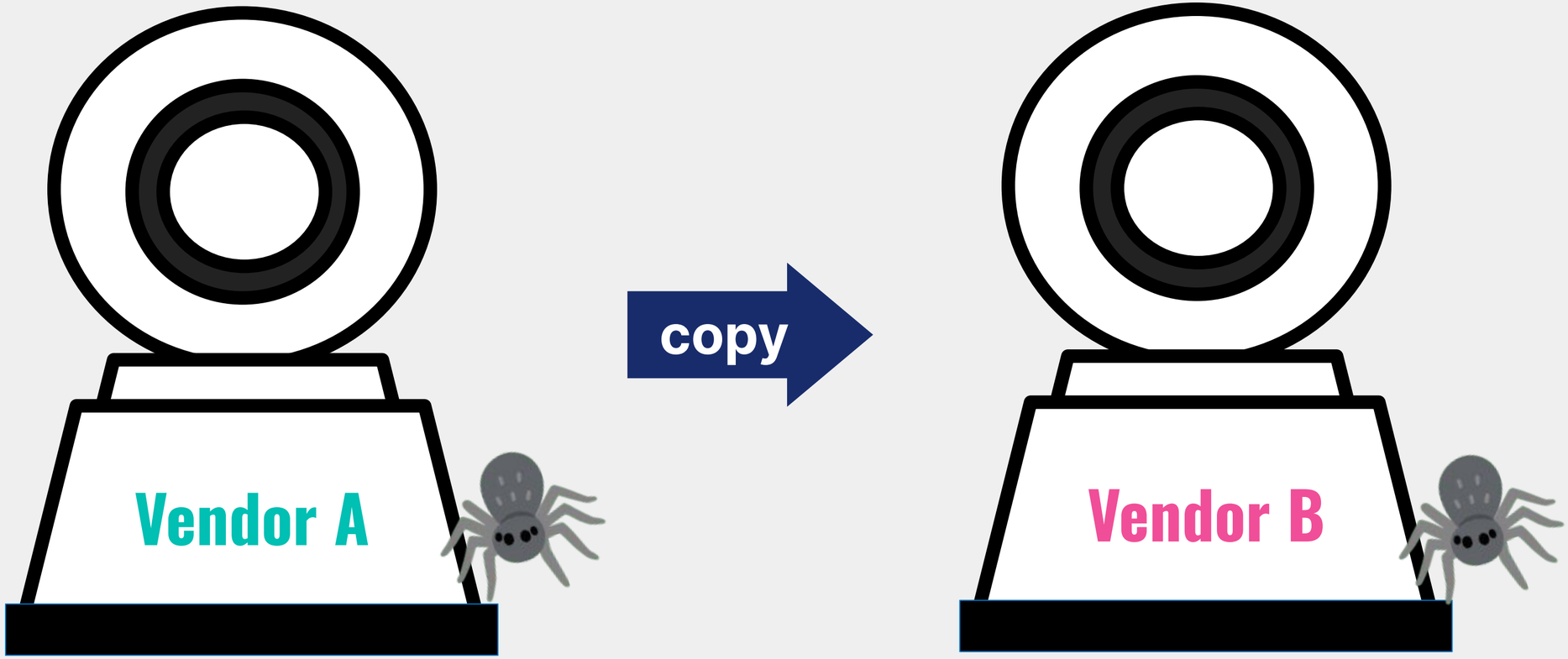


IoT Camera (Original)

IoT Camera (OEM)

Security Risk of OEM Supply Chain

aka White Label Model



IoT Camera (Original)

IoT Camera (OEM)

CVE-2010-4230

copy

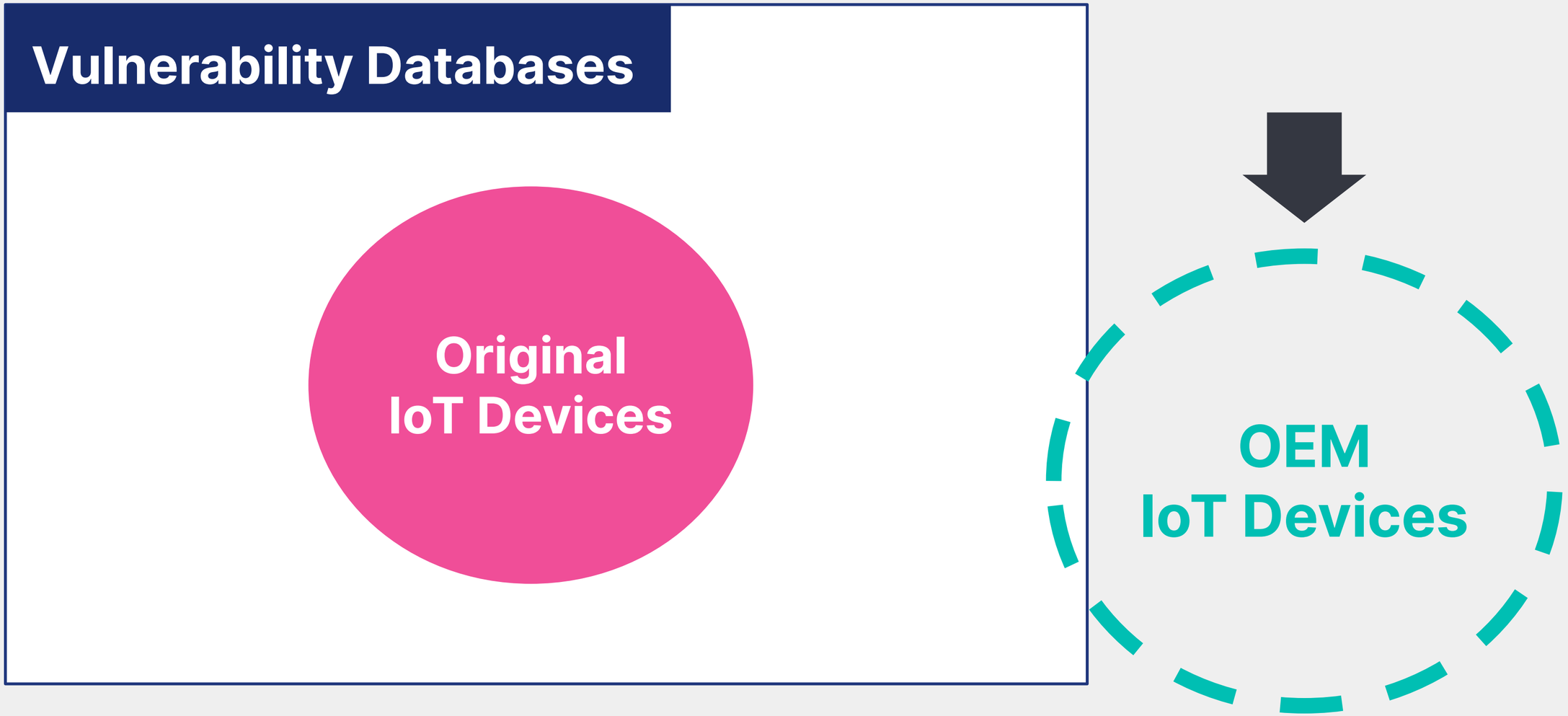
IoT Camera (Original)

Vendor	Camtron
Model	CMNC-200

IoT Camera (OEM)

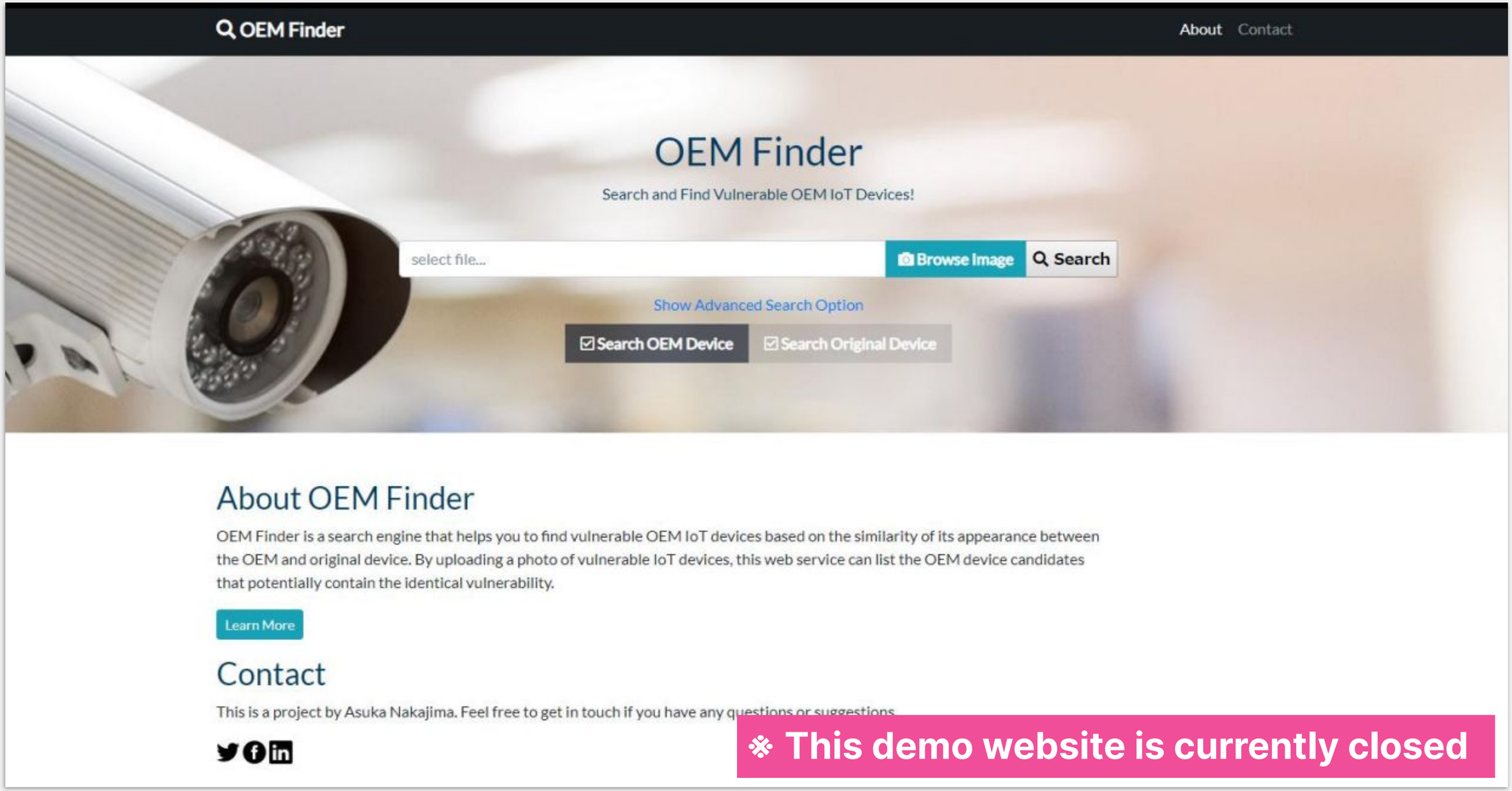
Vendor	Tecvoz
Model	CMNC-200

OEM Devices are NOT Included in Vuln DBs🚫



OEM Device users cannot know about the risks

Created an OEM IoT Device Search Engine

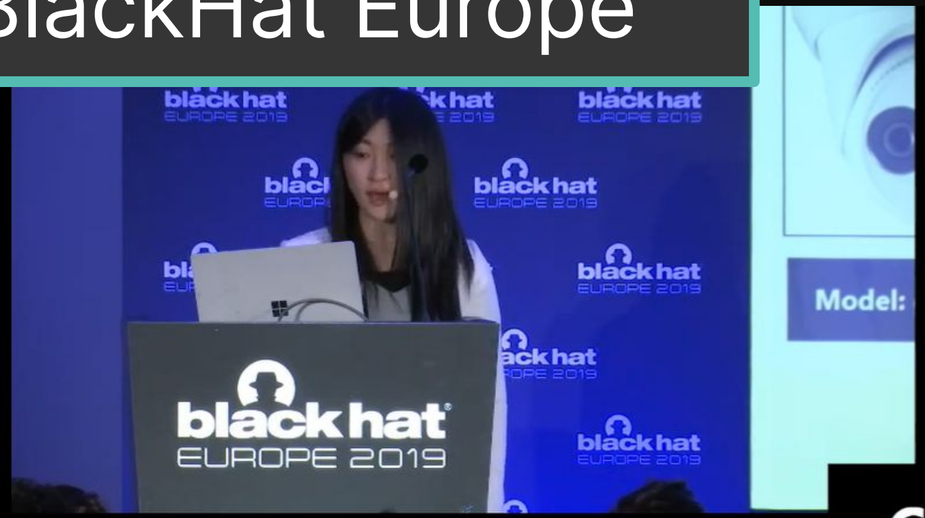


※ This demo website is currently closed

Reference:https://i.blackhat.com/eu-19/Thursday/eu-19-Nakajima-OEM-Finder-Hunting-Vulnerable-OEM-IoT-Devices-At-Scale-2.pdf, p33

Search Result

BlackHat Europe



https://www.youtube.com/watch?v=AgzfII4pHYE

Suchmaschine entdeckt Sicherheitslücken in Security-Kameras

Von *Kristian Kißling* - 05. Dezember 2019

Auf der Black Hat Europe 2019 haben japanische Security-Forscher von NTT eine Online-Suche vorgestellt, mit der sie Sicherheitslücken in No-Name-Security-Kameras leichter entdecken können.

Wer heute eine Netzwerk-basierte Sicherheitskamera kauft, erhält oft unter verschiedenen Namen das gleiche Gerät. Das ist so, weil ein OEM-Hersteller seine Kamera an verschiedene OEM-Anbieter verkauft, die dann ihre Sticker auf das Gerät pappen und es in den Handel bringen. Das aber bringt in puncto Sicherheit gleich mehrere Probleme mit sich.

Oft stecken in der ausgelieferten Firmware des Originalanbieters Sicherheitslücken. Stopft der OEM-Hersteller diese Sicherheitslücken, landen diese Fixes dennoch häufig nicht in den verkauften Geräten der OEM-Anbieter. Zugleich verraten die National Vulnerability Database (NVD) und die Datenbank der Common Vulnerabilities and Exposures (CVE) nicht, in welchen Geräten welcher weiteren Anbieter diese Sicherheitslücken stecken.

Zudem sind auch die OEM-Anbieter nicht wirklich daran interessiert, dass die Kunden erfahren, von dem die Kamera eigentlich stammt. Der OEM-Hersteller ist daher oft nicht offensichtlich. Kaufen Admins solche No-Name-Security-Kameras, müssen sie also selbst herausfinden, wie sicher diese sind. Sie können dazu die Firmware dumpen, den

Einen anderen Weg schlägt die Japanerin Asuka Nakajima vor, die bei NTT als Security-Forscher arbeitet. Sie und ihr

Suchmaschine entdeckt Sicherheitslücken in Security-Kameras

Von *Kristian Kißling* - 05. Dezember 2019

Auf der Black Hat Europe 2019 haben japanische Security-Forscher von NTT eine Online-Suche vorgestellt, der sie Sicherheitslücken in No-Name-Security-Kameras leichter entdecken können.

Wer heute eine Netzwerk-basierte Sicherheitskamera kauft, erhält oft unter verschiedenen Namen das gleiche G
Das ist so, weil ein OEM-Hersteller seine Kamera an verschiedene OEM-Anbieter verkauft, die dann ihre Sticker a
Gerät pappen und es in den Handel bringen. Das aber bringt in puncto Sicherheit gleich mehrere Probleme mit s

Oft stecken in der ausgelieferten Firmware des Originalanbieters Sicherheitslücken. Stopft der OEM-Hersteller di
Sicherheitslücken, landen diese Fixes dennoch häufig nicht in den verkauften Geräten der OEM-Anbieter. Zugleic
verraten die National Vulnerability Database (NVD) und die Datenbank der Common Vulnerabilities and Exposure
(CVE) nicht, in welchen Geräten welcher weiteren Anbieter diese Sicherheitslücken stecken.

Zudem sind auch die OEM-Anbieter nicht wirklich daran interessiert, dass die Kunden erfahren, von dem die Kamera eigentlich stammt. Der OEM-Hersteller ist daher oft nicht offensichtlich. Kaufen Admins solche No-Name-Security-Kameras, müssen sie also selbst herausfinden, wie sicher diese sind. Sie können dazu die Firmware dumpen, den
elle vergleichen.

https://www.linux-magazin.de/news/suchmaschine-entdeckt-sicherheitsluecken-in-security-kameras/

Einen anderen Weg schlägt die Japanerin Asuka Nakajima vor, die bei NTT als Security-Forscher arbeitet. Sie und ihr

11/15/2019
01:00 PM

Black Hat Europe Brings A Bevy of IoT Security Insights

Black Hat Staff
Event Updates

Attend this London event next month for the latest on how security researchers are finding (and solving) security vulnerabilities in all of your favorite Internet-connected devices.

As the year winds down around us, people around the world are spending more time at home, visiting friends and family. Many of those homes are filled
f Things, and at
me opportunity to
learn about the latest IoT security tricks and techniques.

https://www.darkreading.com/black-hat/black-hat-europe-brings-a-bevy-of-iot-security-insights/d/d-id/1336382

LINUX MAGAZIN ONLINE

News Magazin Listings Digitales Abo Videos Blogs Eve

Embedded Linux Kernel Virtualisierung KDE C++ Projekte openSUSE Steam Deb

Administration Desktop Entwicklung Hardware Netzwerk Security Software Szene IT-

Startseite › News › Suchmaschine entdeckt Sicherheitslücken in Security-Kameras

Suchmaschine entdeckt Sicherheitslücken in Security-Kameras

Von *Kristian Kißling* - 05. Dezember 2019

Auf der Black Hat Europe 2019 haben japanische Security-Forscher von NTT eine Online-Suche vorgestellt, der sie Sicherheitslücken in No-Name-Security-Kameras leichter entdecken können.

Wer heute eine Netzwerk-basierte Sicherheitskamera kauft, erhält oft unter verschiedenen Namen das gl
Das ist so, weil ein OEM-Hersteller seine Kamera an verschiedene OEM-Anbieter verkauft, die dann ihre S
Gerät pappen und es in den Handel bringen. Das aber bringt in puncto Sicherheit gleich mehrere Problem

Oft stecken in der ausgelieferten Firmware des Originalanbieters Sicherheitslücken. Stopft der OEM-Herst
Sicherheitslücken, landen diese Fixes dennoch häufig nicht in den verkauften Geräten der OEM-Anbieter.
verraten die National Vulnerability Database (NVD) und die Datenbank der Common Vulnerabilities and E
(CVE) nicht, in welchen Geräten welcher weiteren Anbieter diese Sicherheitslücken stecken.

Zudem sind auch die OEM-Anbieter nicht wirklich daran interessiert, dass die Kunden erfahren, von dem
eigentlich stammt. Der OEM-Hersteller ist daher oft nicht offensichtlich. Kaufen Admins solche No-Name-
Kameras, müssen sie also selbst herausfinden, wie sicher diese sind. Sie können dazu die Firmware dump
elle vergleichen.

https://www.linux-magazin.de/news/suchmaschine-entdeckt-sicherheitsluecken-in-security-kameras/

Einen anderen Weg schlägt die Japanerin Asuka Nakajima vor, die bei NTT als Security-Forscher arbeitet.

DARKReading | SIGN UP FOR OUR NEWSLETTERS

Authors Slideshows Video Tech Library University Security Now Calendar Black Hat News On

THE EDGE | ANALYTICS | ATTACKS / BREACHES | APP SEC | CLOUD | ENDPOINT | IoT | OPERATIONS | PERIMETI

black hat

Black Hat Asia
May 10-13, 2022
Hybrid/Marina Bay Sands, Singapore

Black Hat USA
August 6-11, 202
Las Vegas, NV, U

11/15/2019
01:00 PM

Black Hat Europe Brings A Bevy of IoT Security Insights

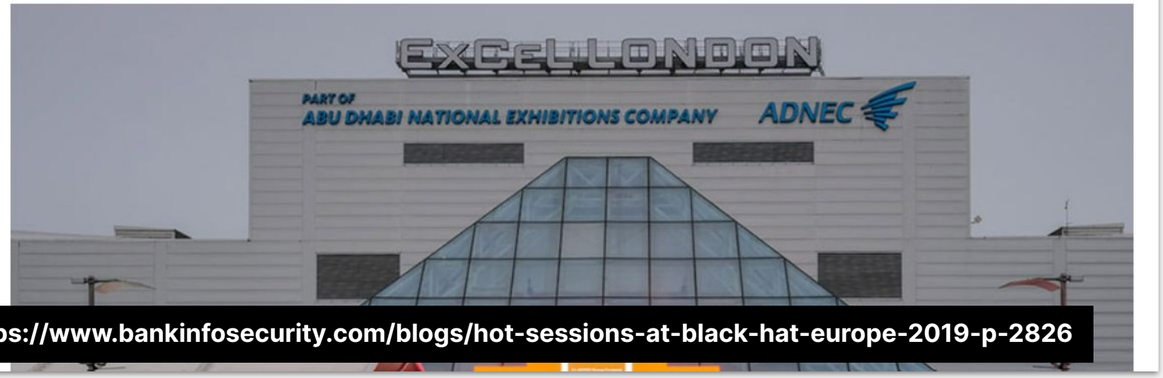
Attend this London event next month for the latest on how security

15 Hot Sessions at Black Hat Europe 2019

Contactless Payments, IoT, False Flag Attacks and More in the Spotlight

Mathew J. Schwartz (euroinfosec) • December 3, 2019

Share Tweet Share Get Permission



https://www.bankinfosecurity.com/blogs/hot-sessions-at-black-hat-europe-2019-p-2826

LINU MAGA

Embedded Linu

Administration

Startseite › News

Suchmasc

Von *Kristian Kißlin*

Auf der Black H
der sie Sicherhe

Wer heute eine N
Das ist so, weil e
Gerät pappen ur

Oft stecken in de
Sicherheitslücke
verraten die Nati
(CVE) nicht, in we

Zudem sind auch
eigentlich stamm
Kameras, müsse

https://www.linux-
herheitsluecken-i

Einen anderen W

NTIA
@NTIAgov

Last week was a big week for #SBOM. NTIA's @allanfriedman spoke at #BSidesSF2020, #CyberTalks, and @RSAConference. You can check out the talk he gave at RSA here: rsaconference.com/usa/agenda/wha...

ポストを翻訳

https://www.bankinfosecurity.com/blogs/hot-sessions-at-black-hat-europe-2019-p-2826

午前3:00 · 2020年3月4日

eading | SIGN UP FOR OUR NEWSLETTERS

deo Tech Library University Security Now Calendar Black Hat News On

TACKS / EACHES | APP SEC | CLOUD | ENDPOINT | IoT | OPERATIONS | PERIMETI

Black Hat Asia
May 10-13, 2022
Hybrid/Marina Bay Sands, Singapore

Black Hat USA
August 6-11, 202
Las Vegas, NV, U

ck Hat Europe Brings A Bevy of Security Insights

this London event next month for the latest on how security

ons at Black Hat Europe 2019

alse Flag Attacks and More in the Spotlight

December 3, 2019

Tweet | Share | Get Permission

com/blogs/hot-sessions-at-black-hat-europe-2019-p-2826

United State's
National Telecommunications and Information Administration

NTIA
@NTIAgov

Last week was a big week for #SBOM. N
#BSidesSF2020, #CyberTalks, and @R
the talk he gave at RSA here: rsaconfere
ポストを翻訳

午前3:00 · 2020年3月4日

"See Asuka Nakajima's OEM Finder"

May 10-13, 2022
Hybrid/Marina Bay Sands, Singapore

August 6-11, 202
Las Vegas, NV, U

ck Hat Europe Brings A Bevy of Security Insights

this London event next month for the latest on how security

ons at Black Hat Europe 2019

alse Flag Attacks and More in the Spotlight

December 3, 2019

Tweet Share Get Permission

ope-2019-p-2826

Embedded Linu
Administration
Startseite › News

Suchmasc

Von *Kristian Kißlin*

**Auf der Black H
der sie Sicherhe**

Wer heute eine N
Das ist so, weil e
Gerät pappen ur

Oft stecken in de
Sicherheitslücke
verraten die Nati
(CVE) nicht, in we

Zudem sind auch
eigentlich stamm
Kameras, müsse

https://www.linux
herheitsluecken-i

Einen anderen W

United State's
National Telecommunications and Information Administration

SBOM (Software Bill of Materials)

https://www.ntia.gov/page/software-bill-materials

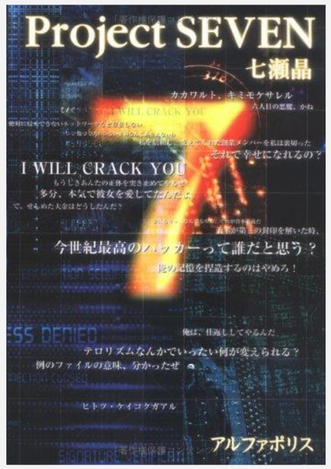
"See Asuka Nakajima's OEM Finder"

Presented at One of the Top Tier Hacker Conferences, and Made a Positive Impact to the World!🌎

Dream has come true?

Timeline

age 14



2004

University Days

DEFCON

2009

Vuln Research

2013

Change the world?

black hat

2019

Rethinking My Career

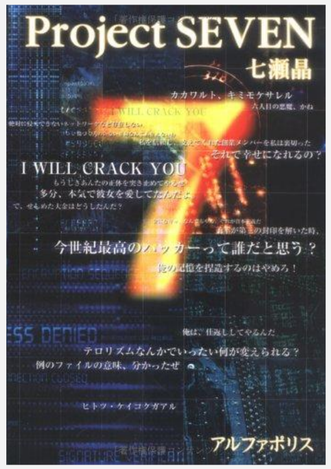
> Although I was able to **make a positive impact on the world** 🌎 through my research, **none of them have been utilized for business or released as tools** 🤔

Rethinking My Career

> Want/Need More **Defence &**
> **Developer Side Experience** to
> Continue Making Positive and
> **Sustainable Impact on the World** 🌎

Timeline

age 14



2004

University Days

DEFCON

2009

Vuln Research

2013

Change the world?

black hat

2019

Defence side!

2022

Endpoint Security R&D (EDR)

EDR: Endpoint Detection and Response

elastic

Elastic Defend

Involved in new feature development which uses Windows ETW

My Journey Continues..

CTF for GIRLS

First Female Infosec Community in Japan

- ✔ Established in **2014**
- ✔ Supported by SECCON
- ✔ Started from about **10** members (now about 50)
- ✔ Hold **Women-Only CTF Workshops** & **CTFs**

CTF for GIRLS

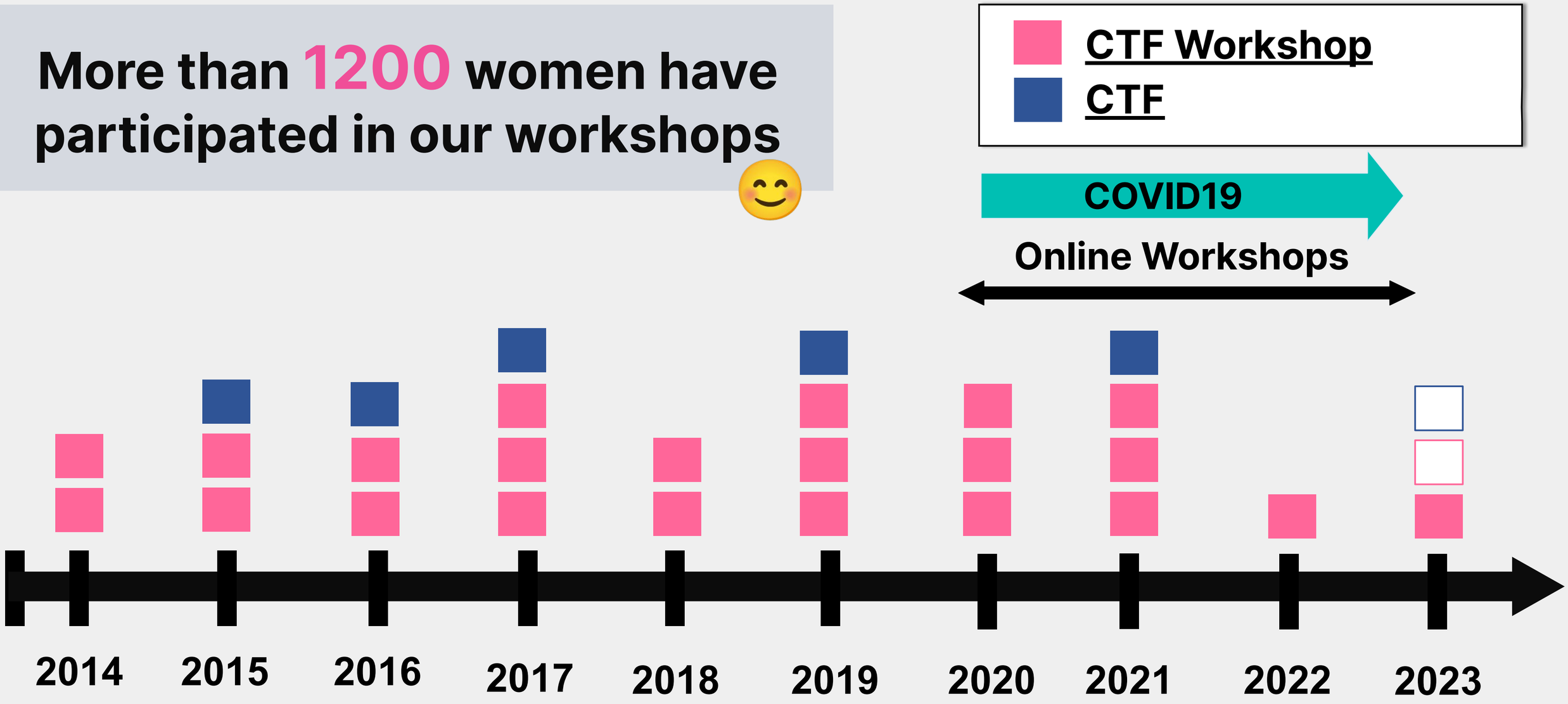
First Workshop was held in June 2014 (Tokyo)

More than **70** people participated in our workshop

Received many **positive feedbacks** from attendees

CTF Workshop (22 times) / CTF (5 times)

More than 1200 women have participated in our workshops 😊



Photos


Post-it
TABLETOP EASEL PAD
TABLEAU À FEUILLES
MODÈLES DE TABLE
3M


Human * IT
人とITのチカラで、驚きと感動のサービスを。
HITACHI
Inspire the Next
株式会社 日立システムズ
CT for GIRLS
日立シ

BlackHat USA 2019

Women in Security:
Building a Female InfoSec Community in Korea, Japan, and Taiwan

HITCON GIRLS
@hitcongirls

We have finished the talk in BlackHat 2019 USA:"
Communities for Women". If any of you are inter
us!

#BHUSA
Asuka Nakajima | #CTFforGIRLS @ctf4g
Suhee Kang | #PowerofXX @POC_Crew
Hazel Yen | #HITCONGIRLS @hitcongirls
ツイートを翻訳

- **Power of XX**
  - Suhee kang (South Korea)
- **CTF for GIRLS**
  - Asuka Nakajima (Japan)
- **HITCON GIRLS**
  - Hazel Yen (Taiwan)

SECCON 2020

Winja × CTF for GIRLS Panel Discussion

- Winja
  - Riddhi Shree (India)
- CTF for GIRLS
  - Asuka Nakajima (Japan)

Winja Meets CTF for GIRLS (CTF4G) | SECCON 2020

Saturday, Dec 19, 2020 winja ctf4g seccon 2020

Representatives of Winja CTF (India) and CTF for GIRLS (Japan) communities had a conversation during SECCON 2020 con

Watch the complete conversation that happened during SECCON 2020 on SECCON YouTube channel:

CTF for GIRLS also provided a CTF challenge for Winja CTF 2021!

Raising Security Awareness

Published **a book📖 called “Cyber Attack”** which talk about software vulnerabilities **to the general public**

Sold about 20000 Copies!😊

Takeaways

#1

#2

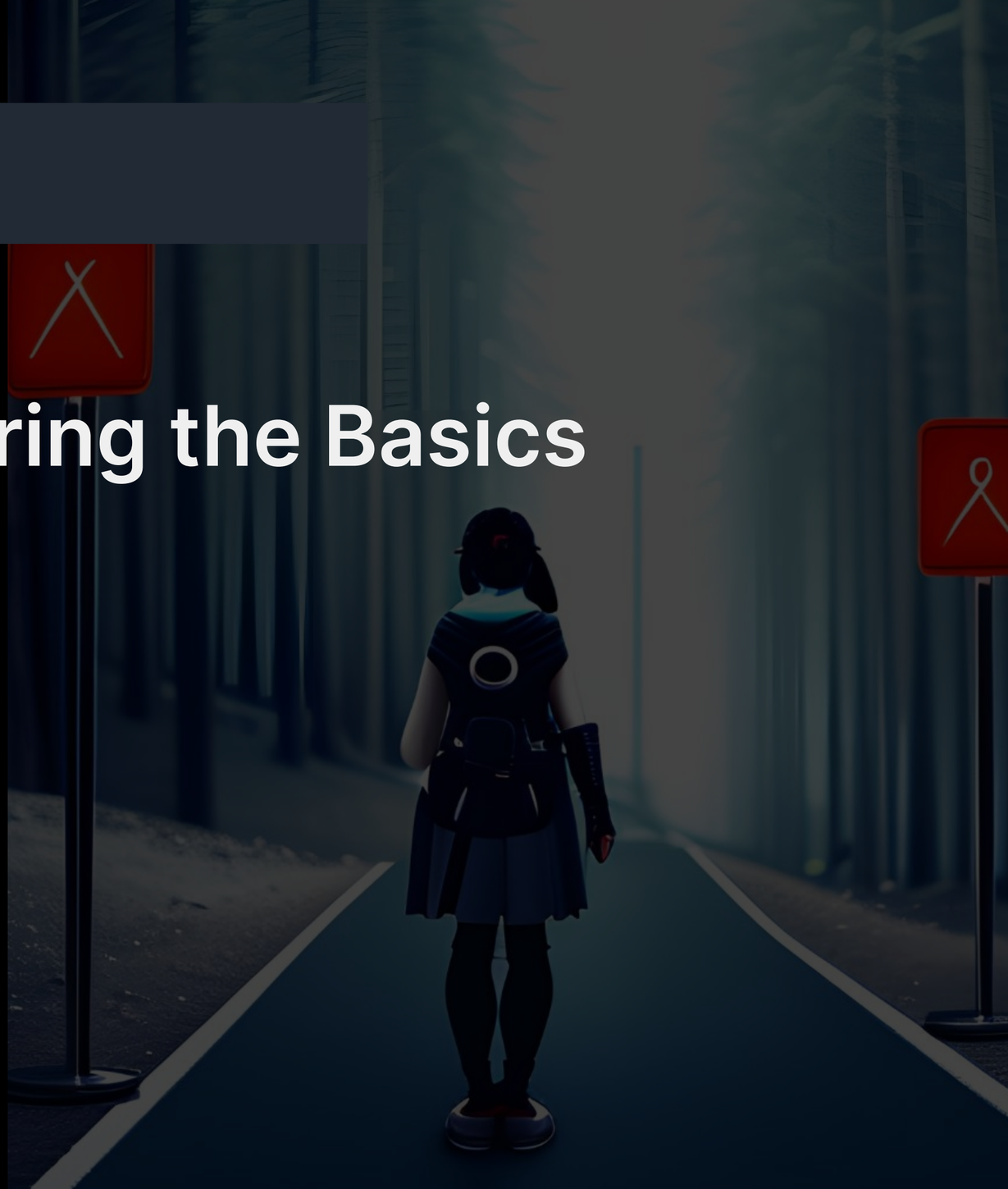
#3

Takeaways

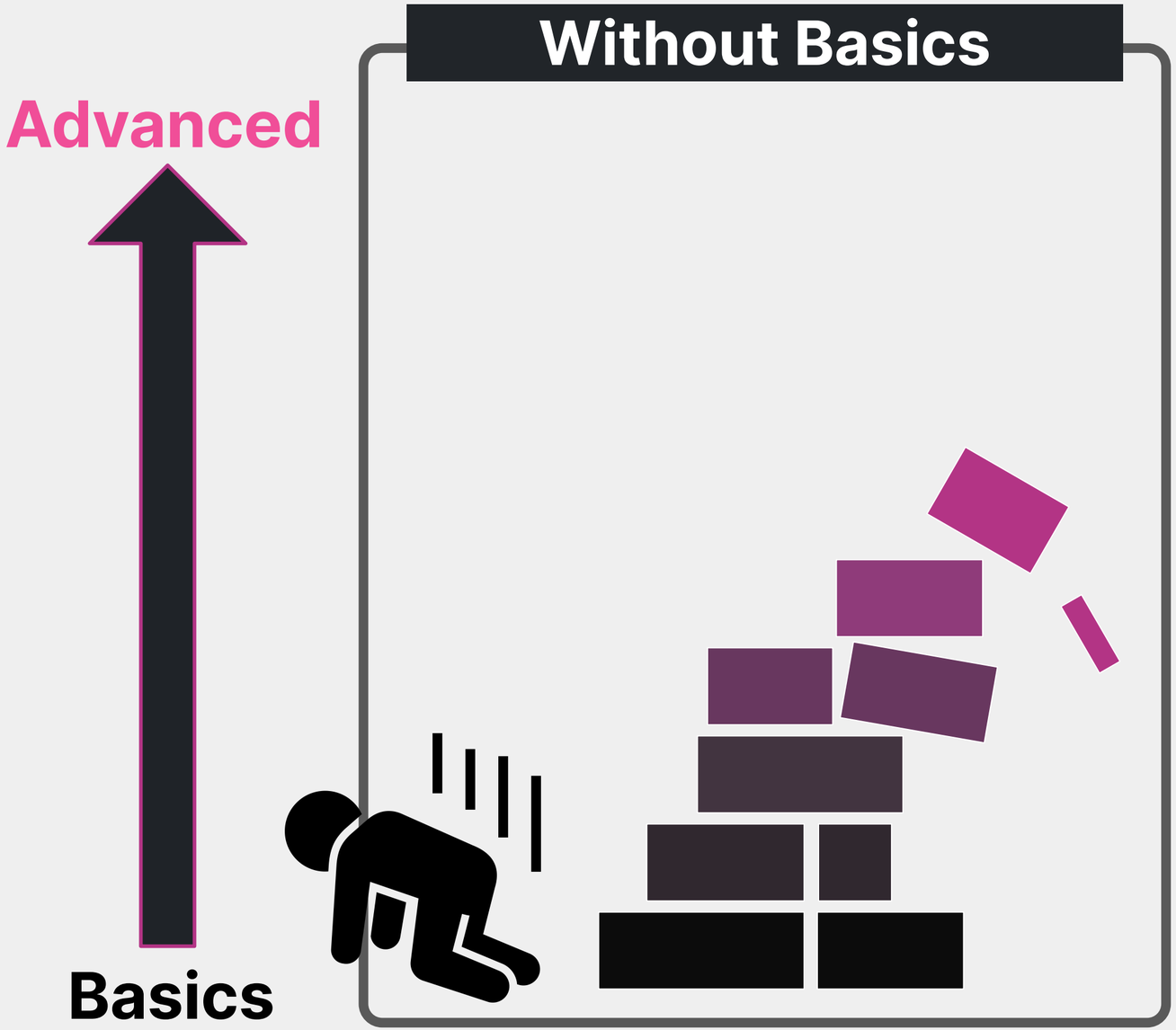
#1 Importance of Mastering the Basics

#2

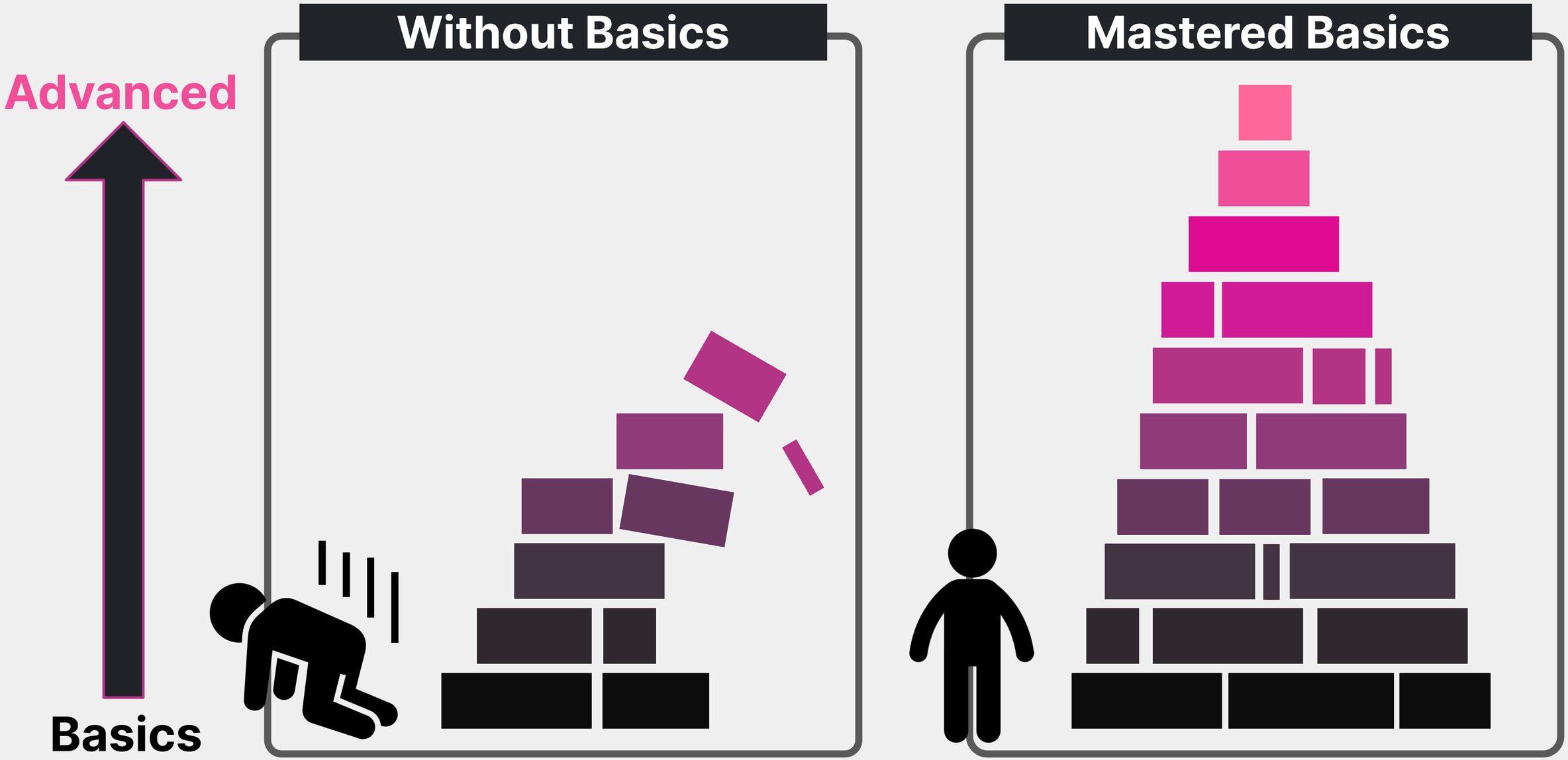
#3



#1 Importance of Mastering the Basics



#1 Importance of Mastering the Basics

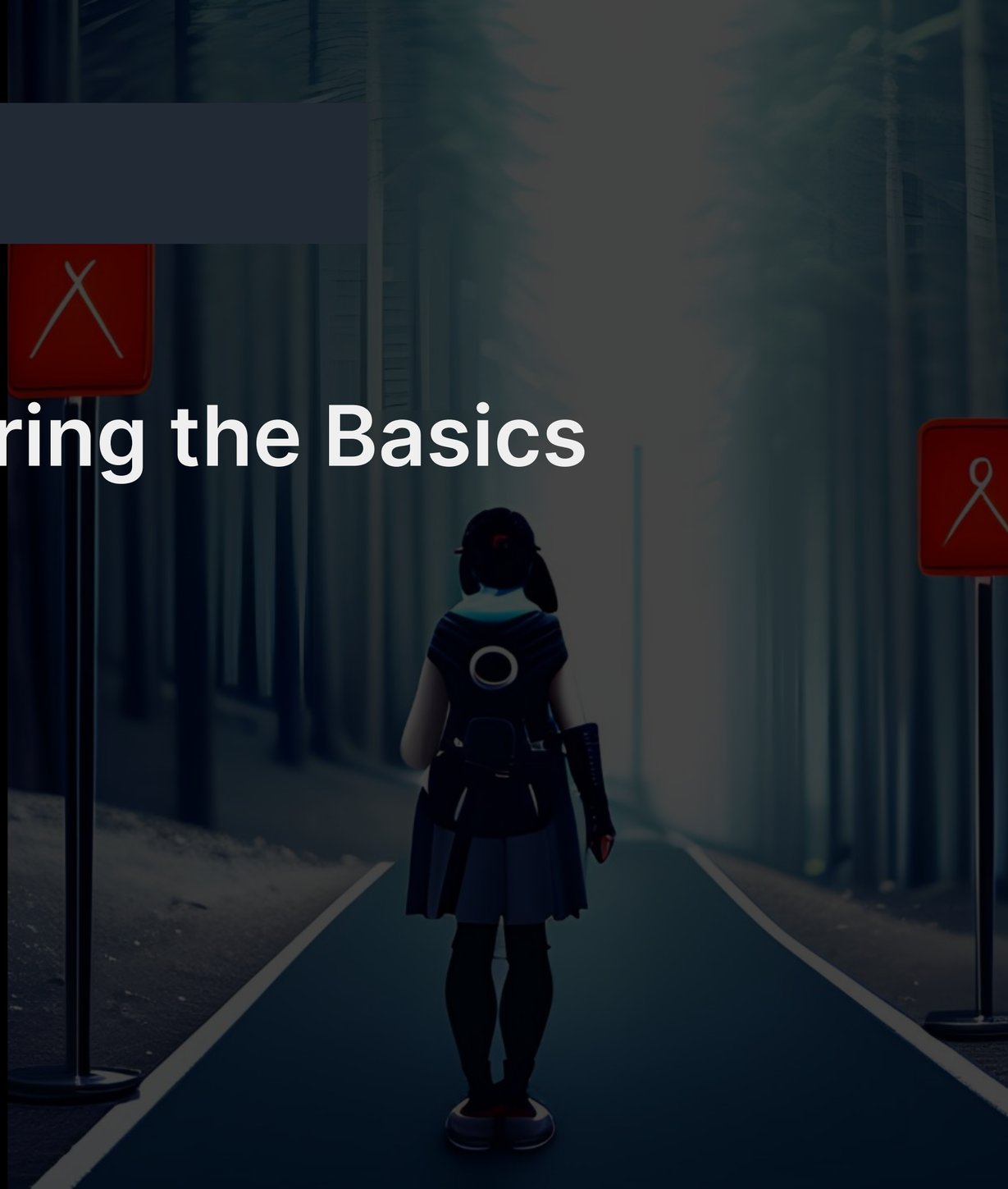


Takeaways

#1 Importance of Mastering the Basics

#2

#3



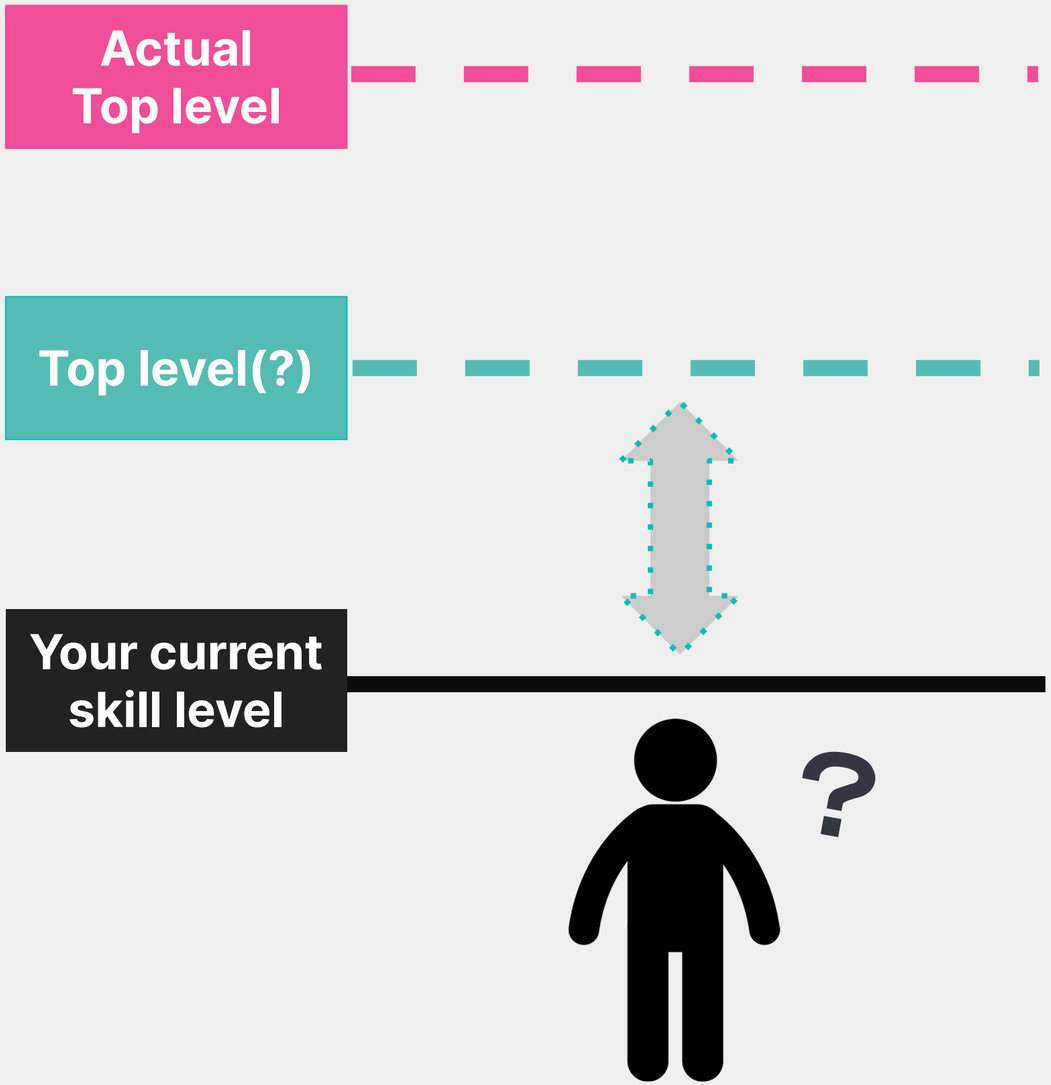
Takeaways

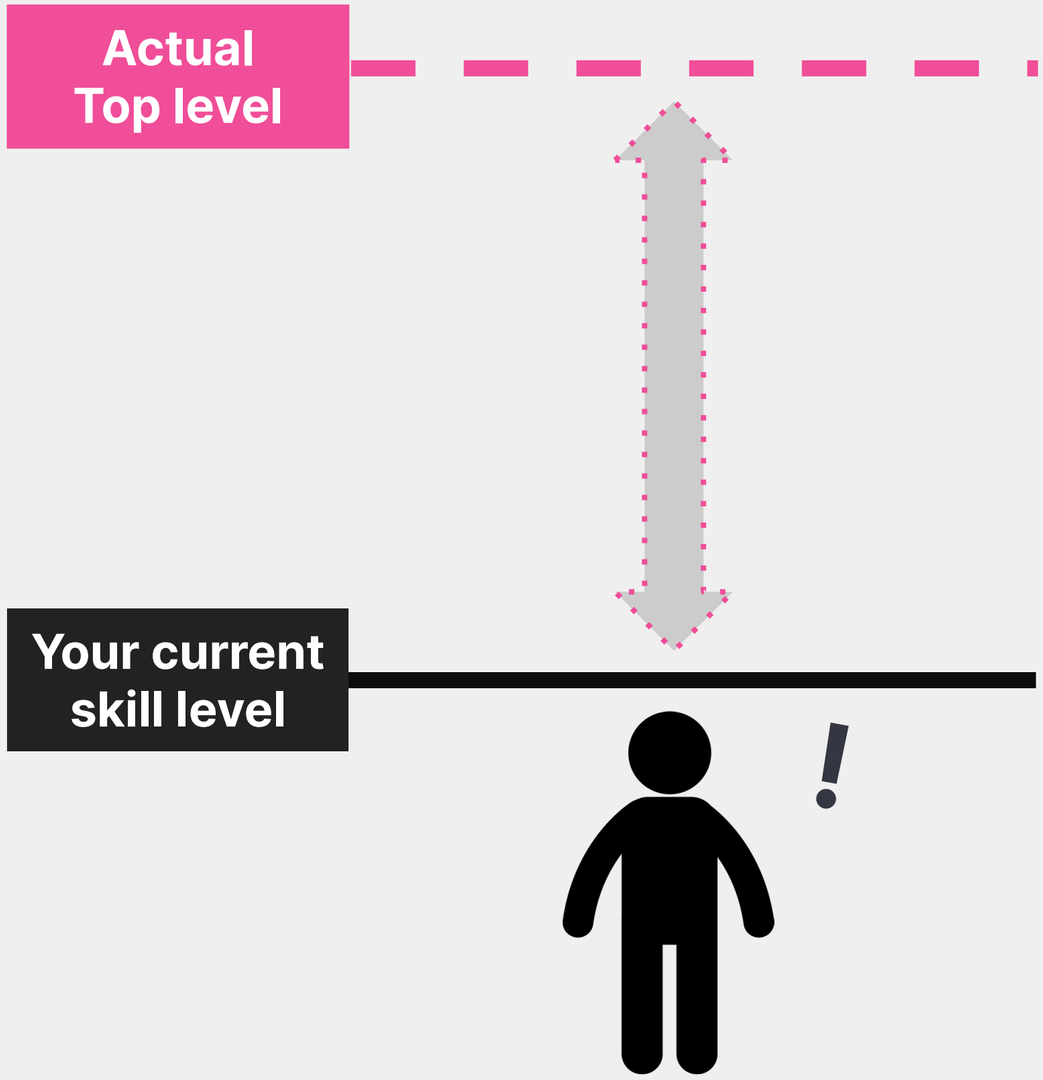
#1 Importance of Mastering the Basics

#2 Understand the Top Level

#3

#2 Understand the Top Level





Takeaways

#1 Importance of Mastering the Basics

#2 Understand the Top Level

#3

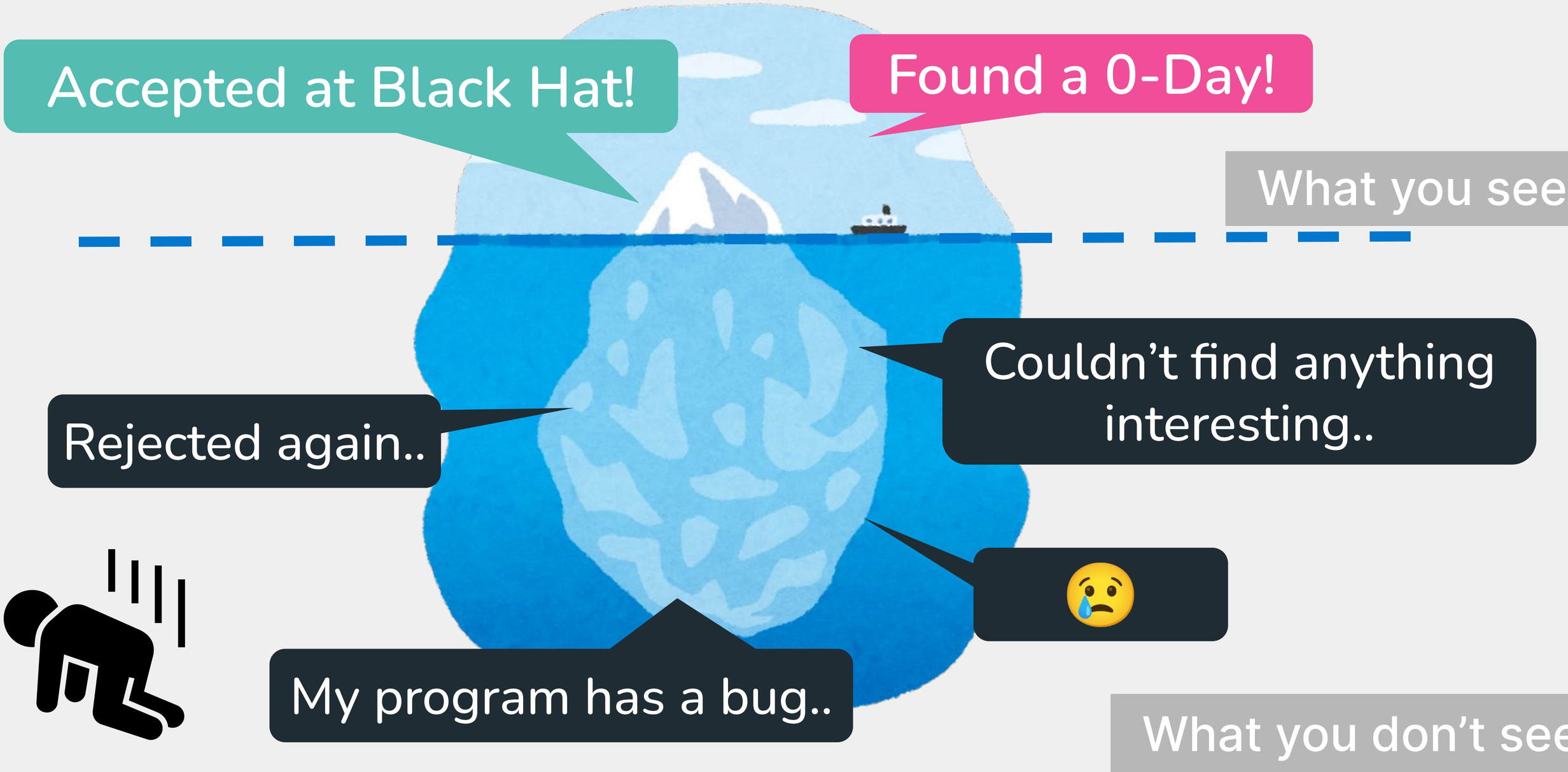
Takeaways

#1 Importance of Mastering the Basics

#2 Understand the Top Level

#3 Keep in Mind that You Won’t Succeed Easily

#3 Keep in Mind that You Won't Succeed Easily



How to Make a Difference

How to Make a Difference

How to Make a Difference

Always Keep in Mind What Value You Can Offer to Others

How to Make a Difference

Always Keep in Mind What Value You Can Offer to Others

Talks about typical stack buffer overflow, but it became a best selling book. Why?🤔

How to Make a Difference

Always Keep in Mind What Value You Can Offer to Others

Talks about typical stack buffer overflow, but it became a best selling book. Why?🤔

There were no books written on such subjects for the general public😲

How to Make a Difference

Always Keep in Mind What Value You Can Offer to Others

Example

Can Provide Information about Trends/Hot Topics in Japan

Let’s Make a Difference, Starting from Here, Today !

Thank you for listening!

E-mail	asuka.nakajima@elastic.co

Website	https://www.kun0ichi.net/
X(Twitter)	@AsuNa_jp
LinkedIn	https://www.linkedin.com/in/asuka-nakajima-89493326/
Facebook	https://www.facebook.com/asuka.nakajima.9